Red Hat Enterprise Linux 9

IdM과 AD 간 신뢰 설치

IdM과 AD 도메인 간 교차 트러스트 관리

Last Updated: 2024-07-23

Red Hat Enterprise Linux 9 IdM과 AD 간 신뢰 설치

IdM과 AD 도메인 간 교차 트러스트 관리

법적 공지

초록

Red Hat IdM(Identity Management) 및 AD(Active Directory)는 모두 Kerberos, LDAP, DNS 및 인증서 서비스와 같은 다양한 핵심 서비스를 관리합니다. 신뢰 관계가 모든 핵심 서비스가 원활하게 상호 작용할 수 있도록 하여 이러한 두 환경을 투명하게 통합합니다. 예를 들어, 신뢰를 통해 AD 사용자는 IdM 토폴로지의 서비스에 인증할 수 있습니다. 신뢰를 준비하려면 IdM 및 AD에서 공통 암호화 유형을 사용하고 방화벽에서 포트를 열고 DNS 및 Kerberos 영역 설정을 구성해야 합니다. 신뢰가 더 이상 필요하지 않은 경우 이를 제거할 수 있습니다.

차례

RED HAT 문서에 관한 피드백 제공

문서에 대한 피드백에 감사드립니다. 어떻게 개선할 수 있는지 알려주십시오.

Jira를 통해 피드백 제출 (등록 필요)

1. Jira 웹 사이트에 로그인합니다.
2. 상단 탐색 모음에서 **생성** 을 클릭합니다.
3. **Summary** (요약) 필드에 설명 제목을 입력합니다.
4. **Description** (설명) 필드에 개선을 위한 제안을 입력합니다. 문서의 관련 부분에 대한 링크를 포함합니다.
5. 대화 상자 하단에서 **생성** 을 클릭합니다.

1장. 신뢰를 설정하기 위한 사전 요구 사항

이 문서에서는 두 서버가 동일한 포리스트에 있는 Identity Management IdM 서버와 Active Directory(AD) 간에 신뢰를 생성하는 데 도움이 됩니다.

사전 요구 사항

- 먼저 Identity Management와 Active Directory 문서 간의 가장 큰 신뢰를 계획 해야 합니다.
- AD는 도메인 컨트롤러와 함께 설치됩니다.
- IdM 서버가 설치되어 실행되고 있습니다.
  자세한 내용은 Identity Management 설치를 참조하십시오.
- Kerberos에는 최대 5분 지연이 필요하므로 AD 서버와 IdM 서버 모두 시계가 동기화되어야 합니다.
- 신뢰에 배치된 각 서버의 고유 name은 Active Directory 도메인을 식별하는 데 중요합니다. Active Directory 또는 IdM 도메인의 이름은 일반적으로 해당 DNS 도메인의 첫 번째 부분입니다. DNS 도메인이 **ad.example.com** 인 경우 일반적으로 이름이 **AD** 입니다. 그러나 필수는 아닙니다. 중요한 것은 이름이 기간이 없는 한 단어로만 발생한다는 것입니다. name의 최대 길이는 15자입니다.
- IdM 시스템에는 커널에서 IPv6 프로토콜이 활성화되어 있어야 합니다.
  IPv6이 비활성화되면 IdM 서비스에서 사용하는 CLDAP 플러그인이 초기화되지 않습니다.

참고

RHEL 7에서는 RHEL 시스템을 AD(Active Directory)에 간접 통합할 수 있는 두 가지 접근 방법이 있었습니다. *RHEL 8에서는 동기화가 더 이상 사용되지 않으며 RHEL 9에서는 더 이상 사용할 수 없습니다. IdM 및 AD를 통합하려면 대신 신뢰 접근 방식을 사용합니다. RHEL 8에서 동기화에서 신뢰로 마이그레이션하려면 기존 환경을 동기화에서 Active Directory 도메인 통합 컨텍스트의 신뢰로 마이그레이션 을 참조하십시오.*

2장. 지원되는 WINDOWS SERVER 버전

다음 포리스트 및 도메인 기능 수준을 사용하는 AD(Active Directory) 포리스트와 신뢰 관계를 설정할 수 있습니다.

- 포리스트 기능 수준 범위: Windows Server 2012 – Windows Server 2016
- 도메인 기능 수준 범위: Windows Server 2012 – Windows Server 2016

IdM(Identity Management)은 다음 운영 체제를 실행하는 Active Directory 도메인 컨트롤러를 통한 신뢰 설정을 지원합니다.

- Windows Server 2022 (RHEL 9.1 이상)
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012

중요

IdM(Identity Management)은 Windows Server 2008 R2 또는 이전 버전을 실행하는 Active Directory 도메인 컨트롤러를 사용하여 Active Directory에 대한 신뢰 설정을 지원하지 않습니다. RHEL IdM에는 Windows Server 2012 이상에서만 지원되는 신뢰 관계를 설정할 때 SMB 암호화가 필요합니다.

3장. 신뢰가 작동하는 방식

Identity Management IdM과 Active Directory (AD) 간의 신뢰는 cross-realm Kerberos 신뢰에 설정됩니다. 이 솔루션은 Kerberos 기능을 사용하여 서로 다른 ID 소스 간에 신뢰를 설정합니다. 따라서 모든 AD 사용자는 다음을 수행할 수 있습니다.

- Linux 시스템 및 리소스에 액세스하려면 로그인합니다.
- SSO(Single Sign-On) 사용.

모든 IdM 오브젝트는 신뢰에서 IdM에서 관리됩니다.

모든 AD 개체는 트러스트에서 AD에서 관리됩니다.All AD objects are managed in AD in the trust.

복잡한 환경에서 단일 IdM 포리스트를 여러 AD 포리스트에 연결할 수 있습니다. 이 설정을 사용하면 조직의 다양한 기능에 대한 작업을 보다 효과적으로 분리할 수 있습니다. AD 관리자는 Linux 인프라를 완전히 제어하는 동안 사용자와 관련된 사용자 및 정책에 중점을 둘 수 있습니다. 이러한 경우 IdM에서 제어하는 Linux 영역은 AD 리소스 도메인 또는 영역과 유사하지만 Linux 시스템과 유사합니다.

AD 관점에서 Identity Management는 하나의 AD 도메인과 별도의 AD 포리스트를 나타냅니다. AD 포리스트 루트 도메인과 IdM 도메인 간 크로스 포리스트 신뢰가 설정된 경우 AD프로브레이션 도메인의 사용자는 IdM 도메인의 Linux 시스템 및 서비스와 상호 작용할 수 있습니다.

참고

신뢰할 수 있는 환경에서 IdM을 사용하면 ID 뷰를 사용하여 IdM 서버의 AD 사용자에 대해 POSIX 속성을 구성할 수 있습니다.

4 장. AD 관리 권한

AD(Active Directory) 와 IdM(Identity Management) 간에 신뢰를 구축하려면 적절한 AD 권한이 있는 AD 관리자 계정을 사용해야 합니다.

이러한 AD 관리자는 다음 그룹 중 하나의 멤버여야 합니다.

- AD 포리스트의 Enterprise Admin 그룹
- Active Directory 에 대한 포리스트 루트 도메인의 도메인 관리자 그룹

추가 리소스

- 엔터프라이즈 관리자에 대한 자세한 내용은 엔터프라이즈 관리자를 참조하십시오.
- 도메인 관리자에 대한 자세한 내용은 도메인 관리자를 참조하십시오.
- AD 신뢰에 대한 자세한 내용은 도메인 및 Forest 트러스트 작업을 참조하십시오 .

5장. AD 및 RHEL 에서 일반적인 암호화 유형 지원 확인

기본적으로 ID 관리는 RC4, AES-128 및 AES-256 Kerberos 암호화 유형을 지원하여 교차 영역 트러스트를 설정합니다. 또한 기본적으로 SSSD 및 Samba Winbind는 RC4, AES-128 및 AES-256 Kerberos 암호화 유형을 지원합니다.

RC4 암호화는 최신 AES-128 및 AES-256 암호화 유형보다 안전하지 않은 것으로 간주되기 때문에 기본적으로 더 이상 사용되지 않고 비활성화되어 있습니다. 반면 AD(Active Directory) 사용자 자격 증명과 AD 도메인 간의 신뢰는 RC4 암호화를 지원하며 모든 AES 암호화 유형을 지원하지 않을 수 있습니다.

일반적인 암호화 유형이 없으면 RHEL 호스트와 AD 도메인 간의 통신이 작동하지 않거나 일부 AD 계정이 인증되지 않을 수 있습니다. 이 상황을 해결하려면 다음 섹션에 설명된 구성 중 하나를 수행합니다.

중요

IdM이 FIPS 모드인 경우 IdM-AD 통합은 RC4 또는 AES HMAC-SHA1 암호화만 지원하는 경우에만 AD로 인해 작동하지 않지만 FIPS 모드의 RHEL 9에서는 기본적으로 AES HMAC-SHA2만 허용합니다. RHEL 9에서 AES HMAC-SHA1 사용을 활성화하려면 **# update-crypto-policies --set FIPS:AD-SUPPORT** 를 입력합니다.

IdM은 Common Criteria 평가 시스템에서만 사용해야 하는 보다 제한적인 **FIPS:OSPP** 암호화 정책을 지원하지 않습니다.

5.1. AD 에서 AES 암호화 활성화(권장)

AD 포리스트의 AD(Active Directory) 도메인 간 신뢰가 강력한 AES 암호화 유형을 지원하는지 확인하려면 다음 Microsoft 문서를 참조하십시오. AD DS: 보안: 신뢰할 수 있는 도메인의 리소스에 액세스할 때 Kerberos "Unsupported etype" 오류

5.2. GPO 를 사용하여 ACTIVE DIRECTORY 의 AES 암호화 유형 활성화

이 섹션에서는 그룹 정책 개체(GPO)를 사용하여 AD(Active Directory)의 AES 암호화 유형을 활성화하는 방법을 설명합니다. IdM 클라이언트에서 Samba 서버를 실행하는 등의 RHEL의 특정 기능에는 이 암호화 유형이 필요합니다.

RHEL은 더 이상 약한 DES 및 RC4 암호화 유형을 지원하지 않습니다.

사전 요구 사항

- 그룹 정책을 편집할 수 있는 사용자로 AD에 로그인되어 있습니다.
- **그룹 정책 관리 콘솔**이 컴퓨터에 설치되어 있습니다.

절차

1. **그룹 정책 관리 콘솔**을 엽니다.
2. **기본 도메인 정책**에서 마우스 오른쪽 버튼으로 클릭하여 **편집**을 선택합니다. **그룹 정책 관리 편집기**가 열립니다.
3. **컴퓨터 구성 → 정책 → Windows 설정 → 보안 설정 → 로컬 정책 → 보안 옵션**으로 이동합니다.
4. **네트워크 보안을 두 번 클릭합니다. Kerberos** 정책에 허용된 암호화 유형을 구성합니다.

5. ***AES256_HMAC_SHA1***을 선택하고 선택적으로 ***Future 암호화 유형***을 선택합니다.
6. ***OK***를 클릭합니다.
7. ***그룹 정책 관리 편집기*** 를 닫습니다.
8. ***기본 도메인 컨트롤러 정책***에 대한 단계를 반복합니다.
9. Windows 도메인 컨트롤러(DC)가 그룹 정책을 자동으로 적용할 때까지 기다립니다. 또는 DC에서 GPO를 수동으로 적용하려면 관리자 권한이 있는 계정을 사용하여 다음 명령을 입력합니다.

```
C:\> gpupdate /force /target:computer
```

5.3. RHEL 에서 RC4 지원 활성화

AD 도메인 컨트롤러에 대한 인증이 수행되는 모든 RHEL 호스트에서 아래 설명된 단계를 완료합니다.

절차

1. ***update-crypto-policies*** 명령을 사용하여 ***DEFAULT*** 암호화 정책과 함께 ***AD-SUPPORT-LEGACY*** 암호화 하위 정책을 활성화합니다.

```
[root@host ~]# update-crypto-policies --set LEGACY:AD-SUPPORT-LEGACY
Setting system policy to LEGACY:AD-SUPPORT-LEGACY
Note: System-wide crypto policies are applied on application start-up.
It is recommended to restart the system for the change of policies
to fully take place.
```

2. 호스트를 다시 시작합니다.

5.4. 추가 리소스

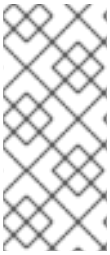
- 전체 시스템 암호화 정책 사용 을 참조하십시오.
- 신뢰 컨트롤러 및 신뢰 에이전트 를 참조하십시오.

6장. IDM과 AD 간의 통신에 필요한 포트

AD(Active Directory)와 IdM(Identity Management) 환경 간 통신을 활성화하려면 AD 도메인 컨트롤러 및 IdM 서버의 방화벽에서 다음 포트를 엽니다.

표 6.1. AD 신뢰에 필요한 포트

Service	포트	프로토콜
끝점 확인 포트 매퍼	135	TCP
NetBIOS-DGM	138	TCP 및 UDP
NetBIOS-SSN	139	TCP 및 UDP
Microsoft-DS	445	TCP 및 UDP
동적 RPC	49152-65535	TCP
AD 글로벌 카탈로그	3268	TCP
LDAP	389	TCP 및 UDP



참고

신뢰를 위해 IdM 서버에서 TCP 포트 389를 열 필요는 없지만 IdM 서버와 통신하는 클라이언트는 필요합니다.

DCE RPC 엔드포인트 매퍼가 작동하려면 TCP 포트 135가 필요하며 IdM-AD 신뢰 생성 중에 사용됩니다.

포트를 열려면 다음 방법을 사용할 수 있습니다.

- ***firewalld** service 인터페이스와 특정 포트를 활성화하거나 포트가 포함된 다음 서비스를 활성화할 수 있습니다.*
  - *FreeIPA 신뢰 설정*
  - *LDAP를 사용하는 FreeIPA*
  - *Kerberos*
  - *DNS*

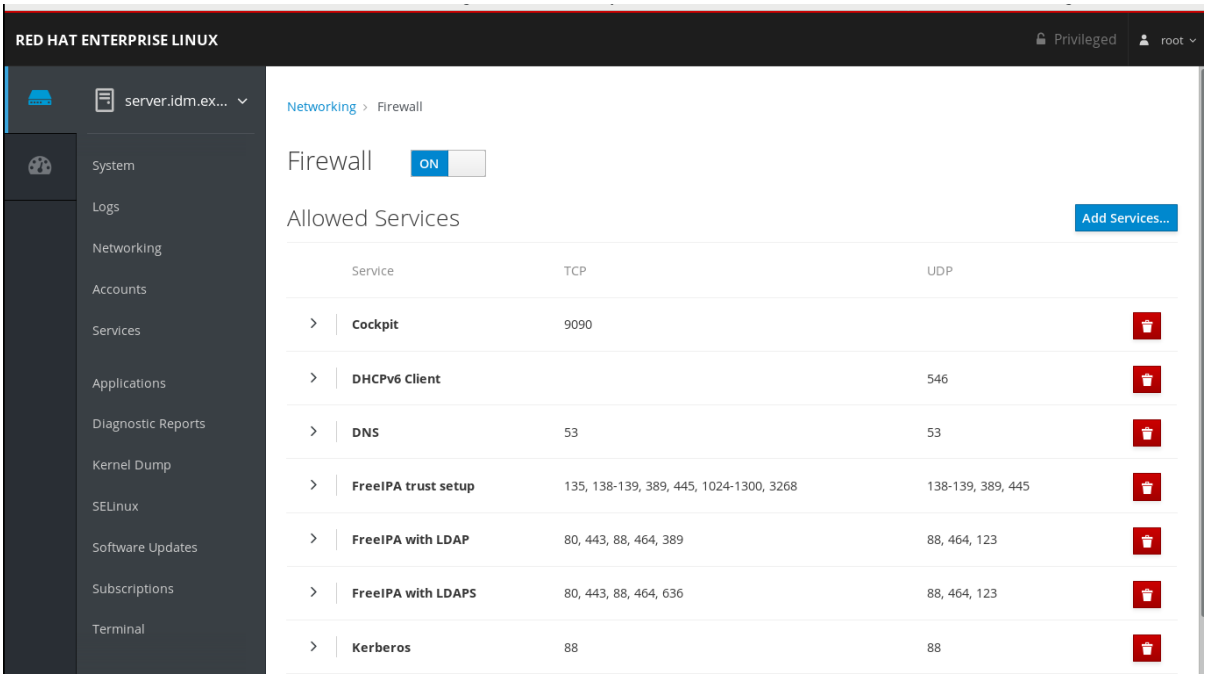
  *자세한 내용은 **firewall-cmd** 도움말 페이지를 참조하십시오.*

참고

RHEL 8.2 및 이전 버전을 사용하는 경우 ***freeipa-trust*** *firewalld 서비스에* ***1024-1300*** *의 RPC 포트 범위가 포함되어 있습니다. 이는 올바르지 않습니다. RHEL 8.2 및 이전 버전에서는* ***freeipa-trust*** *firewalld 서비스를 활성화하는 것 외에도 TCP 포트 범위* ***49152-65535*** *를 수동으로 열어야 합니다.*

이 문제는 RHEL 8.3에서 수정되었으며 버그 1850418에서 나중에 - 올바른 동적 RPC 범위를 포함하도록 freeipa-trust.xml 정의를 업데이트 합니다.

- *RHEL 웹 콘솔:* ***firewalld*** *서비스를 기반으로 하는 방화벽 설정이 있는 UI입니다.*



웹 콘솔을 통한 방화벽 구성에 대한 자세한 내용은 웹 콘솔을 사용하여 방화벽에서 서비스 활성화를 참조하십시오.

참고

RHEL 8.2 및 이전 버전을 사용하는 경우 ***FreeIPA 보안 설정*** *서비스에는* ***1024-1300*** *의 RPC 포트 범위가 포함되어 있으며 이는 올바르지 않습니다. RHEL 8.2 및 이전 버전에서는 RHEL 웹 콘솔에서* ***FreeIPA 보안 설정*** *서비스 활성화 외에 TCP 포트 범위* ***49152-65535*** *를 수동으로 열어야 합니다.*

이 문제는 RHEL 8.3에서 수정되었으며 버그 1850418에서 나중에 - 올바른 동적 RPC 범위를 포함하도록 freeipa-trust.xml 정의를 업데이트 합니다.

표 6.2. 신뢰의 IdM 서버에 필요한 포트

Service	포트	프로토콜
Kerberos	88, 464	TCP 및 UDP
LDAP	389	TCP
DNS	53	TCP 및 UDP

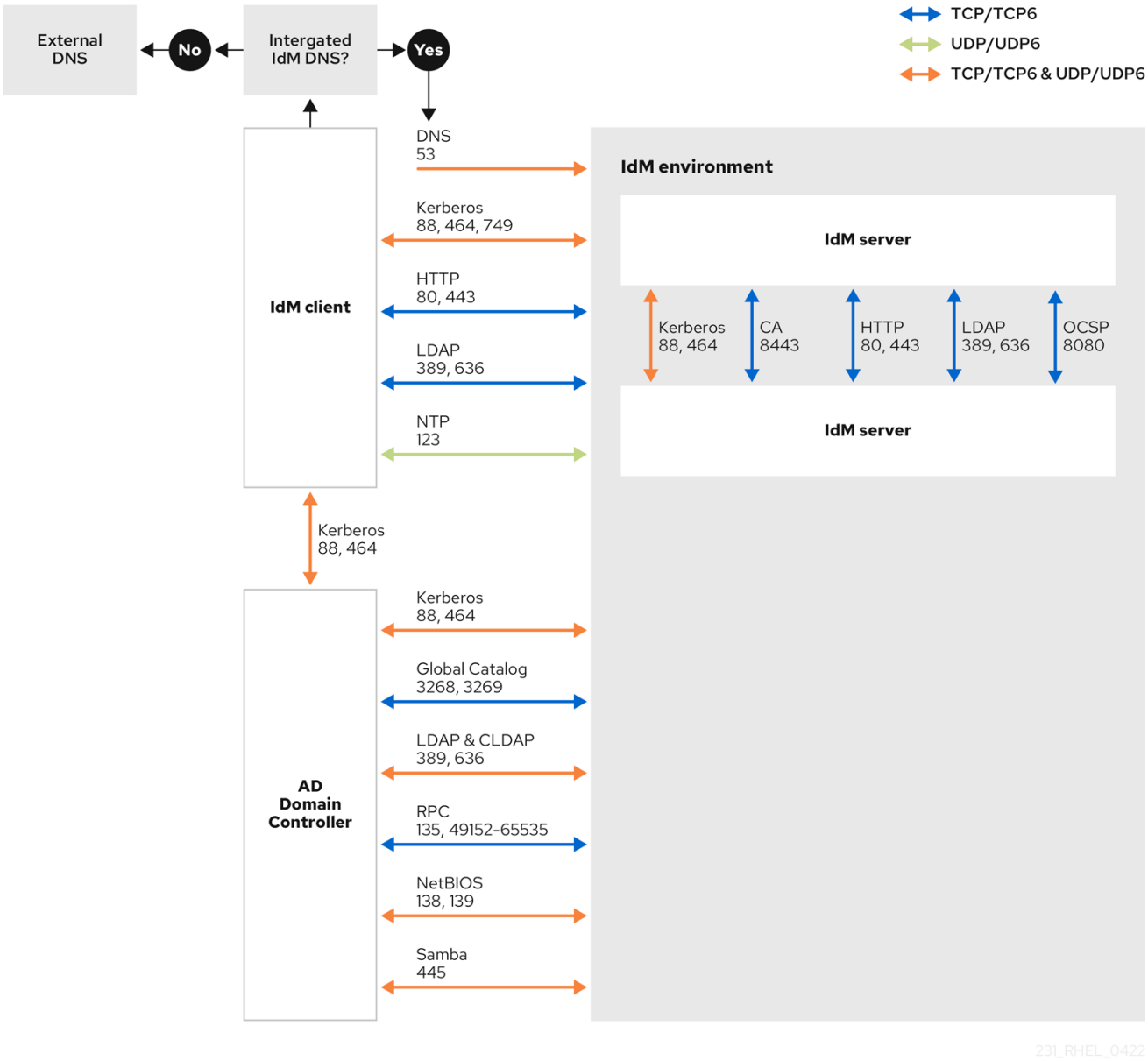
표 6.3. AD 신뢰의 IdM 클라이언트에 필요한 포트

Service	포트	프로토콜
Kerberos	88	UDP 및 TCP

참고

libkrb5 *라이브러리는 UDP를 사용하며 KDC(Key Distribution Center)에서 전송된 데이터가 너무 크면 TCP 프로토콜로 대체됩니다. Active Directory는PAC(권한 속성 인증서)를 Kerberos 티켓에 연결하므로 크기를 늘리고 TCP 프로토콜을 사용해야 합니다. 대체 요청을 방지하고 요청을 재지정하기 위해 기본적으로 Red Hat Enterprise Linux 7.4의 SSSD에서는 사용자 인증에 TCP를 사용합니다.* ***libkrb5*** *가 TCP를 사용하기 전에 크기를 구성하려면* ***/etc/krb5.conf*** *파일에서* ***udp_preference_limit*** *를 설정합니다. 자세한 내용은>-&* ***lt;5.conf(5)*** *매뉴얼 페이지를 참조하십시오.*

다음 다이어그램은 IdM 클라이언트가 전송한 통신을 보여주고 IdM 서버 및 AD 도메인 컨트롤러에서 수신 및 응답하는 방법을 보여줍니다. 방화벽에서 들어오고 나가는 포트 및 프로토콜을 설정하려면 Red Hat에서는 FreeIPA 서비스에 대한 정의가 이미 있는 ***firewalld*** *서비스를 사용하는 것이 좋습니다.*



추가 리소스

- *Windows Server 2008 이상에서 Dynamic RPC 포트 범위에 대한 자세한 내용은 Windows databases 및 Windows Server 2008 이후 TCP/IP의 기본 동적 포트 범위가 변경되었습니다.*

7장. 신뢰에 대한 DNS 및 영역 설정 구성

IdM(Identity Management) 및 AD(Active Directory)를 신뢰에 연결하기 전에 서버가 서로 표시되는지 확인하고 도메인 이름을 올바르게 확인해야 합니다. 다음과 같이 도메인 이름을 사용할 수 있도록 DNS를 구성하려면 다음을 수행합니다.

- 통합된 DNS 서버 및 인증 기관을 사용하는 하나의 기본 IdM 서버.
- AD 도메인 컨트롤러 1개

DNS 설정에는 다음이 필요합니다.

- IdM 서버에서 DNS 영역 구성
- AD에서 조건부 DNS 전달 구성
- DNS 구성의 정확성 확인

7.1. 고유한 기본 DNS 도메인

Windows에서 모든 도메인은 Kerberos 영역과 동시에 DNS 도메인입니다. 도메인 컨트롤러에서 관리하는 모든 도메인에는 자체 전용 DNS 영역이 있어야 합니다. IdM(Identity Management)이 Active Directory(AD)에 의해 포리스트로 신뢰되는 경우에도 마찬가지입니다. AD는 IdM에 자체 DNS 도메인이 있을 것으로 예상합니다. 신뢰 설정이 작동하려면 DNS 도메인이 Linux 환경 전용이어야 합니다.

각 시스템에는 고유한 기본 DNS 도메인이 구성되어 있어야 합니다. 예를 들면 다음과 같습니다.

- AD 및 **idm .example.com for IdM용 ad.example.com**
- IdM의 경우 **example.com** 및 **idm.example.com**
- AD 및 **example .com for IdM의 경우 ad.example.com**

가장 편리한 관리 솔루션은 각 DNS 도메인이 통합된 DNS 서버에서 관리되지만 다른 표준 호환 DNS 서버도 사용할 수 있는 환경입니다.

Kerberos 영역 이름: 기본 DNS 도메인 이름의 대문자 버전

Kerberos 영역 이름은 모든 문자 대문자와 기본 DNS 도메인 이름과 동일해야 합니다. 예를 들어 도메인 이름이 IdM의 **AD 및 idm.example.com** 의 경우 Kerberos 영역 이름은 **AD.EXAMPLE.COM 및 IDM.EXAMPLE.COM** 이어야 합니다.

신뢰의 모든 DNS 도메인에서 DNS 레코드를 확인할 수 있음

모든 시스템은 신뢰 관계에 관련된 모든 DNS 도메인의 DNS 레코드를 확인할 수 있어야 합니다.

IdM 및 AD DNS 도메인

IdM에 연결된 시스템은 여러 DNS 도메인에 배포할 수 있습니다. Red Hat은 Active Directory가 소유한 DNS 영역에 IdM 클라이언트를 배포하는 것이 좋습니다. 기본 IdM DNS 도메인에는 AD 트러스트를 지원하기 위해 적절한 SRV 레코드가 있어야 합니다.

참고

IdM과 Active Directory 간에 신뢰할 수 있는 일부 환경에서는 Active Directory DNS 도메인의 일부인 호스트에 IdM 클라이언트를 설치할 수 있습니다. 그러면 호스트는 Linux 중심 IdM 기능을 활용할 수 있습니다. 이는 권장되는 구성이 아니며 몇 가지 제한 사항이 있습니다. 자세한 내용은 Active Directory DNS 도메인에서 IdM 클라이언트 구성을 참조하십시오.

다음 명령을 실행하여 시스템 설정과 관련된 필요한 SRV 레코드 목록을 가져올 수 있습니다.

```
$ ipa dns-update-system-records --dry-run
```

생성된 목록은 다음과 같이 나타날 수 있습니다.

```
IPA DNS records:
_kerberos-master._tcp.idm.example.com. 86400 IN SRV 0 100 88 server.idm.example.com.
_kerberos-master._udp.idm.example.com. 86400 IN SRV 0 100 88 server.idm.example.com.
_kerberos._tcp.idm.example.com. 86400 IN SRV 0 100 88 server.idm.example.com.
_kerberos._tcp.idm.example.com. 86400 IN SRV 0 100 88 server.idm.example.com.
_kerberos.idm.example.com. 86400 IN TXT "IDM.EXAMPLE.COM"
_kpasswd._tcp.idm.example.com. 86400 IN SRV 0 100 464 server.idm.example.com.
_kpasswd._udp.idm.example.com. 86400 IN SRV 0 100 464 server.idm.example.com.
_ldap._tcp.idm.example.com. 86400 IN SRV 0 100 389 server.idm.example.com.
_ipa-ca.idm.example.com. 86400 IN A 192.168.122.2
```

동일한 IdM 영역에 속하는 다른 DNS 도메인의 경우 AD에 대한 신뢰가 구성될 때 SRV 레코드를 구성할 필요가 없습니다. 이유는 AD 도메인 컨트롤러에서 SRV 레코드를 사용하여 KDC 레코드를 검색하는 대신 신뢰의 이름 접미사 라우팅 정보를 KDC 검색에 기반하기 때문입니다.

7.2. IDM 웹 UI에서 DNS 전달 영역 구성

IdM 웹 UI를 사용하여 IdM(Identity Management) 서버에 DNS 전달 영역을 추가하려면 다음 절차를 따르십시오.

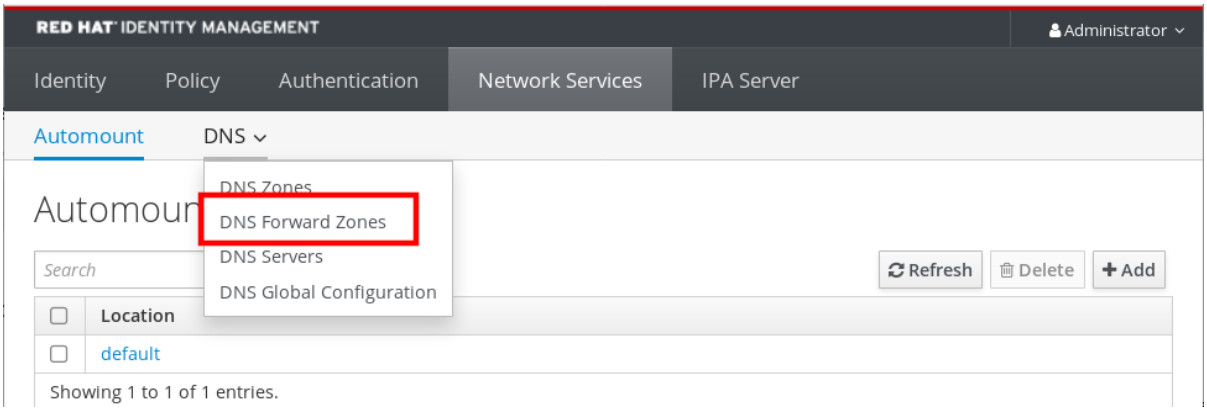
DNS 전달 영역을 사용하면 특정 영역의 DNS 쿼리를 다른 DNS 서버로 전달할 수 있습니다. 예를 들어 AD(Active Directory) 도메인에 대한 DNS 쿼리를 AD DNS 서버로 전달할 수 있습니다.

사전 요구 사항

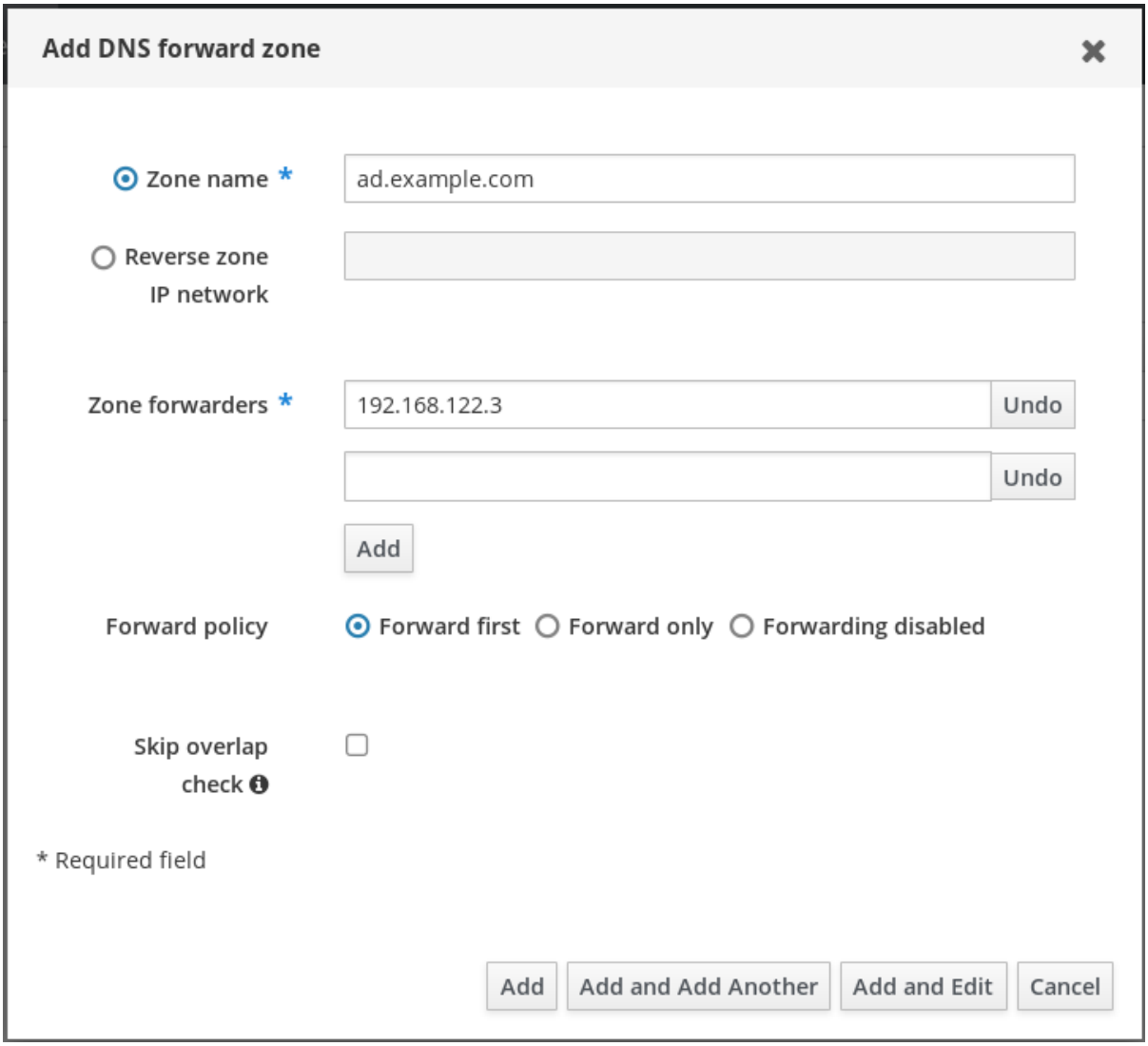
- 관리자 권한이 있는 사용자 계정으로 IdM 웹 UI에 액세스합니다.
- DNS 서버가 올바르게 구성되어 있습니다.

절차

1. 관리자 권한으로 IdM 웹 UI에 로그인합니다. 자세한 내용은 웹 브라우저에서 IdM 웹 UI 액세스를 참조하십시오.
2. **네트워크 서비스** 탭을 클릭합니다.
3. **DNS** 탭을 클릭합니다.
4. 드롭다운 메뉴에서 **DNS 전달 영역** 항목을 클릭합니다.



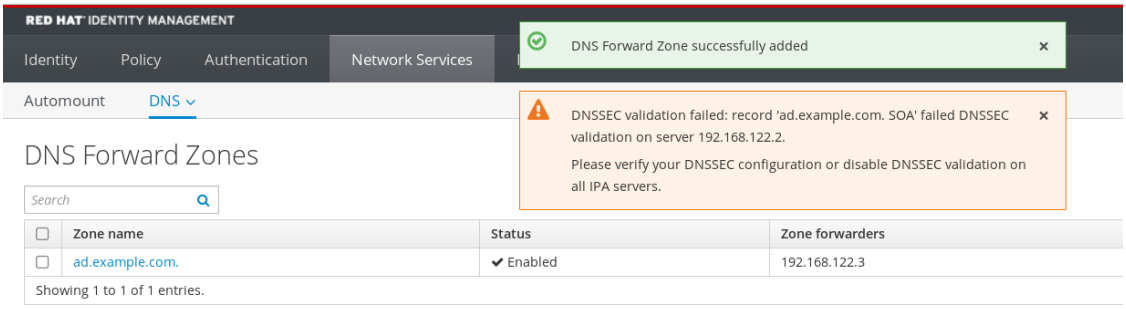
5. *추가 버튼을 클릭합니다.*
6. ***DNS 전달 영역 추가** 대화 상자에서 영역 이름을 추가합니다.*
7. ***Zone forwarders** 항목에서 **Add** 버튼을 클릭합니다.*
8. ***Zone forwarders** 필드에서 전달 영역을 생성할 서버의 IP 주소를 추가합니다.*
9. *추가 버튼을 클릭합니다.*



*전달된 영역이 DNS 설정에 추가되어 DNS 전달 영역에서 확인할 수 있습니다. 웹 UI는 다음과 같은 팝업 메시지를 사용하여 성공에 대해 알려줍니다. **DNS 전달 영역이 추가되었습니다.***

참고

Web UI는 전달 영역을 구성에 추가한 후 DNSSEC 검증 실패에 대한 경고를 표시할 수 있습니다.



DNSSEC (Domain Name System Security Extensions)는 공격으로부터 DNS를 보호하기 위해 디지털 서명으로 DNS 데이터를 보호합니다. 이 서비스는 IdM 서버에서 기본적으로 활성화되어 있습니다. 원격 DNS 서버에서 DNSSEC를 사용하지 않기 때문에 경고가 표시됩니다. 원격 DNS 서버에서 DNSSEC를 활성화하는 것이 좋습니다.

원격 서버에서 DNSSEC 검증을 활성화할 수 없는 경우 IdM 서버에서 DNSSEC를 비활성화할 수 있습니다.

1. *편집할 적절한 구성 파일을 선택합니다.*
   - *IdM 서버에서 RHEL 8.0 또는 RHEL 8.1을 사용하는 경우 **/etc/named.conf** 파일을 엽니다.*
   - *IdM 서버에서 RHEL 8.2 이상을 사용하는 경우 **/etc/named/ipa-options-ext.conf** 파일을 엽니다.*
2. *다음 DNSSEC 매개변수를 추가합니다.*

```
dnssec-enable no;
dnssec-validation no;
```

3. *구성 파일을 저장한 후 닫습니다.*
4. *DNS 서비스를 다시 시작하십시오.*

```
# systemctl restart named-pkcs11
```

검증 단계

- *원격 DNS 서버의 이름과 함께 **nslookup** 명령을 사용합니다.*

```
$ nslookup ad.example.com
Server:         192.168.122.2
Address:        192.168.122.2#53

No-authoritative answer:
Name:           ad.example.com
Address:        192.168.122.3
```

도메인 전달을 올바르게 구성한 경우 원격 DNS 서버의 IP 주소가 표시됩니다.

7.3. CLI에서 DNS 전달 영역 구성

CLI(명령줄 인터페이스)를 사용하여 IdM(Identity Management) 서버에 새 DNS 전달 영역을 추가하려면 다음 절차를 따르십시오.

DNS 전달 영역을 사용하면 특정 영역의 DNS 쿼리를 다른 DNS 서버로 전달할 수 있습니다. 예를 들어 AD(Active Directory) 도메인에 대한 DNS 쿼리를 AD DNS 서버로 전달할 수 있습니다.

사전 요구 사항

- 관리자 권한이 있는 사용자 계정으로 CLI에 액세스합니다.
- DNS 서버가 올바르게 구성되어 있습니다.

절차

- AD 도메인의 DNS 전달 영역을 생성하고 **--forwarder** 옵션을 사용하여 원격 DNS 서버의 IP 주소를 지정합니다.

```
# ipa dnsforwardzone-add ad.example.com --forwarder=192.168.122.3 --forward-policy=first
```

참고

구성에 새 전달 영역을 추가한 후 **/var/log/messages** 시스템 로그에서 DNSSEC 검증 실패에 대한 경고가 표시될 수 있습니다.

```
named-pkcs11[2572]: no valid DS resolving 'host.ad.example.com/A/IN':
192.168.100.25#53
```

DNSSEC (Domain Name System Security Extensions)는 공격으로부터 DNS를 보호하기 위해 디지털 서명으로 DNS 데이터를 보호합니다. 이 서비스는 IdM 서버에서 기본적으로 활성화되어 있습니다. 원격 DNS 서버에서 DNSSEC를 사용하지 않기 때문에 경고가 표시됩니다. 원격 DNS 서버에서 DNSSEC를 활성화하는 것이 좋습니다.

원격 서버에서 DNSSEC 검증을 활성화할 수 없는 경우 IdM 서버에서 DNSSEC를 비활성화할 수 있습니다.

1. **/etc/named/ipa-options-ext.conf** 파일을 엽니다.
2. 다음 DNSSEC 매개변수를 추가합니다.

```
dnssec-enable no;
dnssec-validation no;
```

3. 구성 파일을 저장한 후 닫습니다.
4. DNS 서비스를 다시 시작하십시오.

```
# systemctl restart named-pkcs11
```

검증 단계

- 원격 DNS 서버의 이름과 함께 **nslookup** 명령을 사용합니다.

```
$ nslookup ad.example.com
Server:         192.168.122.2
Address:        192.168.122.2#53

No-authoritative answer:
Name:           ad.example.com
Address:        192.168.122.3
```

도메인 전달이 올바르게 구성된 경우 ***nslookup*** *요청에 원격 DNS 서버의 IP 주소가 표시됩니다.*

7.4. AD 에서 DNS 전달 구성

IdM(Identity Management) 서버의 AD(Active Directory) 에서 DNS 전달을 설정하려면 다음 절차를 따르십시오.

사전 요구 사항

- *AD 가 설치된 Windows Server*
- *두 서버에서 모두 DNS 포트가 열려 있습니다.*

절차

1. *Windows Server 에 로그인합니다.*
2. ***Server Manager*** *를 엽니다.*
3. ***DNS 관리자를*** *엽니다.*
4. ***Conditional Forwarders*** *에서 다음을 사용하여 새 조건부 전달자를 추가합니다.*
   - *IdM 서버 IP 주소*
   - *정규화된 도메인 이름(예:* ***server.idm.example.com****)*
5. *설정을 저장합니다.*

7.5. DNS 구성 확인

신뢰를 구성하기 전에 IdM(Identity Management) 및 AD(Active Directory) 서버가 서로 확인할 수 있는지 확인합니다.

사전 요구 사항

- *sudo 권한으로 로그인해야 합니다.*

절차

1. *UDP 를 통한 Kerberos 및 TCP 서비스 레코드를 통해 LDAP 에 대한 DNS 쿼리를 실행합니다.*

```
[admin@server ~]# dig +short -t SRV _kerberos._udp.idm.example.com.
0 100 88 server.idm.example.com.
```

```
[admin@server ~]# dig +short -t SRV _ldap._tcp.idm.example.com.
0 100 389 server.idm.example.com.
```

명령에는 모든 IdM 서버가 나열되어야 합니다.

2. IdM Kerberos 영역 이름으로 TXT 레코드에 대한 DNS 쿼리를 실행합니다. 얻은 값은 IdM을 설치할 때 지정한 Kerberos 영역과 일치해야 합니다.

```
[admin@server ~]# dig +short -t TXT _kerberos.idm.example.com.
"IDM.EXAMPLE.COM"
```

이전 단계에서 예상되는 모든 레코드를 반환하지 않으면 누락된 레코드로 DNS 구성을 업데이트합니다.

- IdM 환경에서 통합 DNS 서버를 사용하는 경우 시스템 레코드를 업데이트할 옵션 없이 **ipa dns-update-system-annotations 명령을** 입력합니다.

```
[admin@server ~]$ ipa dns-update-system-records
```

- IdM 환경에서 통합 DNS 서버를 사용하지 않는 경우:

  1. IdM 서버에서 IdM DNS 레코드를 파일로 내보냅니다.

```
[admin@server ~]$ ipa dns-update-system-records --dry-run --out
dns_records_file.nsupdate
```

이 명령은 관련 IdM DNS 레코드를 **사용하여 dns_annotations_file.nsupdate** 라는 파일을 생성합니다.

  2. **nsupdate 유틸리티 및 dns_file.nsupdate** 파일을 사용하여 DNS 서버에 DNS 업데이트 요청을 제출합니다. 자세한 내용은 RHEL 7 설명서에서 nsupdate를 사용하여 외부 DNS 레코드 업데이트에서 참조하십시오. 또는 DNS 레코드를 추가하기 위한 DNS 서버 설명서를 참조하십시오.

3. IdM이 Kerberos 및 TCP 서비스 레코드를 통해 LDAP에 대한 DNS 쿼리를 실행하는 명령을 사용하여 AD의 서비스 레코드를 확인할 수 있는지 확인합니다.

```
[admin@server ~]# dig +short -t SRV _kerberos._tcp.dc._msdcs.ad.example.com.
0 100 88 addc1.ad.example.com.

[admin@server ~]# dig +short -t SRV _ldap._tcp.dc._msdcs.ad.example.com.
0 100 389 addc1.ad.example.com.
```

8 장. ACTIVE DIRECTORY DNS 도메인에서 IDM 클라이언트 구성

Active Directory가 관리하는 DNS 도메인에 클라이언트 시스템이 있고 해당 클라이언트가 RHEL 기능을 활용하기 위해 IdM 서버에 연결해야 하는 경우, Active Directory DNS 도메인에서 호스트 이름을 사용하여 클라이언트에 액세스하도록 사용자를 구성할 수 있습니다.

중요

이는 권장되는 구성이 아니며 몇 가지 제한 사항이 있습니다. Red Hat은 항상 Active Directory가 소유한 DNS 영역에 IdM 클라이언트를 배포하고 IdM 호스트 이름을 통해 IdM 클라이언트에 액세스할 것을 권장합니다.

IdM 클라이언트 구성은 Kerberos로 SSO(Single Sign-On)가 필요한지 여부에 따라 달라집니다.

8.1. KERBEROS SSO(SINGLE SIGN-ON)가 없는 IDM 클라이언트 구성

암호 인증은 IdM 클라이언트가 Active Directory DNS 도메인에 있는 경우 사용자가 IdM 클라이언트의 리소스에 액세스할 수 있는 유일한 인증 방법입니다. Kerberos Single Sign-On 없이 클라이언트를 구성하려면 다음 절차를 따르십시오.

절차

1. SSSD(System Security Services Daemon)가 IdM 서버와 통신할 수 있도록 **--domain=IPA_DNS_Domain** 옵션으로 IdM 클라이언트를 설치합니다.

```
[root@idm-client.ad.example.com ~]# ipa-client-install --domain=idm.example.com
```

   이 옵션은 Active Directory DNS 도메인에 대한 SRV 레코드 자동 감지를 비활성화합니다.

2. **/etc/krb5.conf** 구성 파일을 열고 **[domain_realm]** 섹션에서 Active Directory 도메인의 기존 매핑을 찾습니다.

```
.ad.example.com = IDM.EXAMPLE.COM
ad.example.com = IDM.EXAMPLE.COM
```

3. 두 행을 Active Directory DNS 영역에 있는 Linux 클라이언트의 FQDN(정규화된 도메인 이름)과 IdM 영역을 매핑하는 항목으로 바꿉니다.

```
idm-client.ad.example.com = IDM.EXAMPLE.COM
```

   기본 매핑을 대체하면 Kerberos가 Active Directory 도메인에 대한 요청을 IdM Kerberos 배포 센터(KDC)로 전송하지 못합니다. 대신 Kerberos는 SRV DNS 레코드를 통한 자동 검색을 사용하여 KDC를 찾습니다.

8.2. SINGLE SIGN-ON 없이 SSL 인증서 요청

SSL 기반 서비스에는 원래(A/AAAA)와 CNAME 레코드가 모두 인증서에 있어야 하므로 모든 시스템 호스트 이름을 포함하는 **dNSName** 확장 레코드가 있는 인증서가 필요합니다. 현재 IdM은 IdM 데이터베이스의 오브젝트를 호스트하는 인증서만 발행합니다.

Single Sign-On을 사용할 수 없는 설명된 설정에서 IdM에는 데이터베이스에 FQDN의 호스트 오브젝트가 이미 있으며 **certmonger** 는 이 이름을 사용하여 인증서를 요청할 수 있습니다.

사전 요구 사항

- Kerberos Single Sign-On 없이 IdM 클라이언트 구성 절차에 따라 IdM 클라이언트 설치 및 구성.

절차

- **certmonger** 를 사용하여 FQDN을 사용하여 인증서를 요청합니다.

```
[root@idm-client.ad.example.com ~]# ipa-getcert request -r \
    -f /etc/httpd/alias/server.crt \
    -k /etc/httpd/alias/server.key \
    -N CN=ipa-client.ad.example.com \
    -D ipa-client.ad.example.com \
    -K host/idm-client.ad.example.com@IDM.EXAMPLE.COM \
    -U id-kp-serverAuth
```

certmonger 서비스는 **/etc/krb5.keytab** 파일에 저장된 기본 호스트 키를 사용하여 IdM CA(인증 기관)에 인증합니다.

8.3. KERBEROS SSO(SINGLE SIGN-ON)를 사용하여 IDM 클라이언트 구성

IdM 클라이언트의 리소스에 액세스하기 위해 Kerberos Single Sign-on이 필요한 경우 클라이언트는 IdM DNS 도메인(예: **idm-client.idm.example.com**) 내에 있어야 합니다. IdM 클라이언트의 A/AAAA 레코드를 가리키는 Active Directory DNS 도메인에 CNAME 레코드 **idm-client.ad.example.com** 을 생성해야 합니다.

Kerberos 기반 애플리케이션 서버의 경우 MIT Kerberos는 애플리케이션의 키 탭에서 사용 가능한 호스트 기반 주체를 수락할 수 있는 방법을 지원합니다.

절차

- IdM 클라이언트에서 **/etc/krb5.conf 구성 파일의 [libdefaults] 섹션에 다음 옵션을 설정하여 Kerberos 주체가 Kerberos 서버를 대상으로 하는 데 사용되는 엄격한 검사를 비활성화합니다.**

```
ignore_acceptor_hostname = true
```

8.4. SINGLE SIGN-ON으로 SSL 인증서 요청

SSL 기반 서비스에는 원래(A/AAAA)와 CNAME 레코드가 모두 인증서에 있어야 하므로 모든 시스템 호스트 이름을 포함하는 **dNSName** 확장 레코드가 있는 인증서가 필요합니다. 현재 IdM은 IdM 데이터베이스의 오브젝트를 호스트하는 인증서만 발행합니다.

다음 절차에 따라 IdM에서 **ipa-client.example.com** 에 대한 호스트 오브젝트를 생성하고 실제 IdM 시스템의 호스트 오브젝트가 이 호스트를 관리할 수 있는지 확인합니다.

사전 요구 사항

- Kerberos Single Sign-On으로 IdM 클라이언트 구성에 설명된 대로 Kerberos 주체가 Kerberos 서버를 대상으로 하는 데 사용되는 사항에 대한 엄격한 검사를 비활성화했습니다.

절차

1. IdM 서버에 새 호스트 오브젝트를 생성합니다.

```
[root@idm-server.idm.example.com ~]# ipa host-add idm-client.ad.example.com --force
```

호스트 이름은 A/AAAA 레코드가 아닌 CNAME이므로 ***--force*** *옵션을 사용합니다.*

2. *IdM 서버에서 IdM DNS 호스트 이름이 IdM 데이터베이스의 Active Directory 호스트 항목을 관리할 수 있도록 허용합니다.*

```
[root@idm-server.idm.example.com ~]# ipa host-add-managedby idm-client.ad.example.com \
    --hosts=idm-client.idm.example.com
```

3. *이제 Active Directory DNS 도메인 내의 호스트 이름에 대해* ***dNSName*** *확장 레코드를 사용하여 IdM 클라이언트의 SSL 인증서를 요청할 수 있습니다.*

```
[root@idm-client.idm.example.com ~]# ipa-getcert request -r \
    -f /etc/httpd/alias/server.crt \
    -k /etc/httpd/alias/server.key \
    -N CN=`hostname --fqdn` \
    -D `hostname --fqdn` \
    -D idm-client.ad.example.com \
    -K host/idm-client.idm.example.com@IDM.EXAMPLE.COM \
    -U id-kp-serverAuth
```

9장. 신뢰 설정

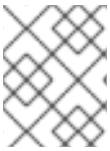
이 섹션에서는 명령줄을 사용하여 IdM 측에서 IdM(Identity Management)/Active Directory(AD) 트러스트를 구성하는 방법을 설명합니다.

사전 요구 사항

- DNS가 올바르게 구성되어 있습니다. IdM 및 AD 서버 모두 서로 이름을 확인할 수 있어야 합니다. 자세한 내용은 신뢰의 DNS 및 영역 설정 구성을 참조하십시오 .
- 지원되는 AD 및 IdM 버전이 배포됩니다. 자세한 내용은 지원되는 Windows Server 버전을 참조하십시오.
- Kerberos 티켓을 받았습니다. 자세한 내용은 kinit를 사용하여 IdM에 수동으로 로그인합니다.

9.1. 신뢰를 위한 IDM 서버 준비

AD를 사용하여 신뢰를 구축하기 전에 IdM 서버에서 **ipa-adtrust-install** 유틸리티를 사용하여 IdM 도메인을 준비해야 합니다.



참고

ipa-adtrust-install 명령을 자동으로 실행하는 시스템은 AD 신뢰 컨트롤러가 됩니다. 그러나 IdM 서버에서 **ipa-adtrust-install** 을 한 번만 실행해야 합니다.

사전 요구 사항

- IdM 서버가 설치되어 있어야 합니다.
- 패키지를 설치하고 IdM 서비스를 다시 시작하려면 루트 권한이 필요합니다.

절차

1. 필수 패키지를 설치합니다.

```
[root@ipaserver ~]# dnf install ipa-server-trust-ad samba-client
```

2. IdM 관리자로 인증합니다.

```
[root@ipaserver ~]# kinit admin
```

3. **ipa-adtrust-install** 유틸리티를 실행합니다.

```
[root@ipaserver ~]# ipa-adtrust-install
```

IdM이 통합된 DNS 서버와 함께 설치된 경우 DNS 서비스 레코드가 자동으로 생성됩니다.

통합된 DNS 서버 없이 IdM을 설치한 경우, **ipa-adtrust-install** 은 DNS에 수동으로 추가해야 하는 서비스 레코드 목록을 인쇄합니다.

4. 스크립트에서 **/etc/samba/smb.conf** 가 이미 존재하고 다시 작성됨을 묻는 메시지를 표시합니다.

```
WARNING: The smb.conf already exists. Running ipa-adtrust-install will break your existing
```

```
Samba configuration.

Do you wish to continue? [no]: yes
```

5. 스크립트에서 이전 Linux 클라이언트가 신뢰할 수 있는 사용자로 작업할 수 있는 호환성 플러그인인 **slapi-nis** 플러그인을 구성하도록 프롬프트를 표시합니다.

```
Do you want to enable support for trusted domains in Schema Compatibility plugin?
This will allow clients older than SSSD 1.9 and non-Linux clients to work with trusted users.

Enable trusted domains support in slapi-nis? [no]: yes
```

6. SID 생성 작업을 실행하여 기존 사용자의 SID를 생성하라는 메시지가 표시됩니다.

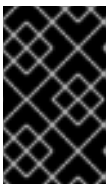
```
Do you want to run the ipa-sidgen task? [no]: yes
```

이는 리소스 집약적인 작업이므로 사용자가 많은 경우 한 번에 이 작업을 실행할 수 있습니다.

7. **(선택 사항)** 기본적으로 Dynamic RPC 포트 범위는 Windows Server 2008 이상에서는 **49152-65535** 로 정의됩니다. 환경에 대해 다른 Dynamic RPC 포트 범위를 정의해야 하는 경우 다른 포트를 사용하도록 Samba를 구성하고 방화벽 설정에서 해당 포트를 엽니다. 다음 예제에서는 포트 범위를 **55000-65000**으로 설정합니다.

```
[root@ipaserver ~]# net conf setparm global 'rpc server dynamic port range' 55000-65000
[root@ipaserver ~]# firewall-cmd --add-port=55000-65000/tcp
[root@ipaserver ~]# firewall-cmd --runtime-to-permanent
```

8. 신뢰의 DNS 구성 확인에 설명된 대로 DNS가 올바르게 구성되었는지 확인합니다 .



중요

ipa-adtrust-install 을 실행한 후 언제든지 DNS 구성 확인에 설명된 대로 DNS 구성을 확인하는 것이 좋습니다(특히 IdM 또는 AD에서 통합 DNS 서버를 사용하지 않는 경우).

9. **ipa** 서비스를 다시 시작하십시오.

```
[root@ipaserver ~]# ipactl restart
```

10. **smbclient** 유틸리티를 사용하여 Samba가 IdM 측에서 Kerberos 인증에 응답하는지 확인합니다.

```
[root@ipaserver ~]# smbclient -L ipaserver.idm.example.com -U user_name --use-kerberos=required
lp_load_ex: changing to config backend registry
    Sharename       Type      Comment
    ---------       ----      -------
    IPC$            IPC       IPC Service (Samba 4.15.2)
...
```

9.2. 명령줄을 사용하여 신뢰 계약 설정

명령줄을 사용하여 신뢰 계약을 설정하려면 다음 절차를 따르십시오. IdM(Identity Management) 서버를 사용하면 세 가지 유형의 신뢰 계약을 구성할 수 있습니다.

- **One-way trust** expects. 단방향 신뢰로 인해 AD(Active Directory) 사용자 및 그룹이 IdM의 리소스에 액세스할 수 있지만 다른 방법은 액세스할 수 없습니다. IdM 도메인은 AD 포리스트를 신뢰하지만 AD 포리스트에서는 IdM 도메인을 신뢰하지 않습니다.

- **양방향 trust expect: Two-**way trust를 통해 AD 사용자 및 그룹이 IdM의 리소스에 액세스할 수 있습니다.
  S4U2Self 및 S4U2 Proxy Microsoft 확장에서 신뢰할 수 있는 경계를 통해 작동하도록 Microsoft SQL Server와 같은 솔루션에 대한 양방향 신뢰를 구성해야 합니다. RHEL IdM 호스트의 애플리케이션은 AD 사용자에 대한 Active Directory 도메인 컨트롤러에서 **S4U2Self 또는 S4U2Proxy** 정보를 요청할 수 있으며 양방향 신뢰에서는 이 기능을 제공합니다.

  이 양방향 신뢰 기능은 IdM 사용자가 Windows 시스템에 로그인할 수 없으며 IdM의 양방향 신뢰는 사용자에게 AD의 단방향 신뢰 솔루션에 비해 추가 권한을 부여하지 않습니다.

  - 양방향 신뢰를 생성하려면 명령에 다음 옵션을 추가합니다. **--two-way=true**

- **외부 신뢰** - 다른 포리스트의 IdM과 AD 도메인 간의 신뢰 관계입니다. 포리스트 신뢰는 항상 IdM과 Active Directory 포리스트의 루트 도메인 간 신뢰를 구축해야 하지만 외부 신뢰는 IdM에서 포리스트 내 도메인으로 외부 트러스트를 설정할 수 있습니다. 이는 관리 또는 조직의 이유로 인해 포리스트 루트 도메인 간에 포리스트의 신뢰를 설정할 수 없는 경우에만 권장됩니다.

  - 외부 신뢰를 생성하려면 명령에 다음 옵션을 추가합니다. **--external=true**

아래 단계에서는 단방향 신뢰 계약을 생성하는 방법을 보여줍니다.

사전 요구 사항

- Windows 관리자의 사용자 이름 및 암호입니다.
- 신뢰를 위해 IdM 서버를 준비했습니다.

절차

- **ipa trust-add 명령을 사용하여 AD 도메인 및 IdM 도메인에 대한 신뢰** 계약을 생성합니다.

  - SSSD를 사용하여 STS를 기반으로 AD 사용자의 UID 및 GID를 자동으로 생성할 수 있도록 하려면 **Active Directory 도메인** ID 범위 유형과의 신뢰 계약을 생성합니다. 가장 일반적인 구성입니다.

    ```
    [root@server ~]# ipa trust-add --type=ad ad.example.com --admin
    <ad_admin_username> --password --range-type=ipa-ad-trust
    ```

  - Active Directory에서 사용자에 대한 POSIX 속성을 구성하고(예: **uidNumber** 및 **gidNumber**) SSSD에서 이 정보를 처리하려면 **POSIX 특성 ID 범위 유형을 사용하여 Active Directory 도메인과** 의 신뢰 계약을 생성하십시오.

    ```
    [root@server ~]# ipa trust-add --type=ad ad.example.com --admin
    <ad_admin_username> --password --range-type=ipa-ad-trust-posix
    ```

주의

트러스트를 생성할 때 ID 범위 유형을 지정하지 않으면 IdM에서 포리스트 루트 도메인의 AD 도메인 컨트롤러에서 세부 정보를 요청하여 적절한 범위 유형을 자동으로 선택합니다. IdM에서 POSIX 속성을 감지하지 않으면 신뢰 설치 스크립트에서 ***Active Directory 도메인*** *ID 범위를 선택합니다.*

IdM이 포리스트 루트 도메인에서 POSIX 속성을 감지하면 신뢰 설치 스크립트에서 ***POSIX 속성 ID 범위가 있는 Active Directory 도메인*** *을 선택하고 UID 및 GID가 AD에 올바르게 정의되어 있다고 가정합니다. AD에서 POSIX 속성이 올바르게 설정되지 않은 경우 AD 사용자를 확인할 수 없습니다.*

예를 들어, IdM 시스템에 대한 액세스가 필요한 사용자 및 그룹이 프리브릭 루트 도메인의 일부가 아닌 포리스트 도메인의 하위 도메인에 있는 경우 설치 스크립트에서 하위 AD 도메인에 정의된 POSIX 속성을 감지하지 못할 수 있습니다. 이 경우 신뢰를 설정할 때 POSIX ID 범위 유형을 명시적으로 선택하는 것이 좋습니다.

9.3. IDM 웹 UI에서 신뢰 계약 설정

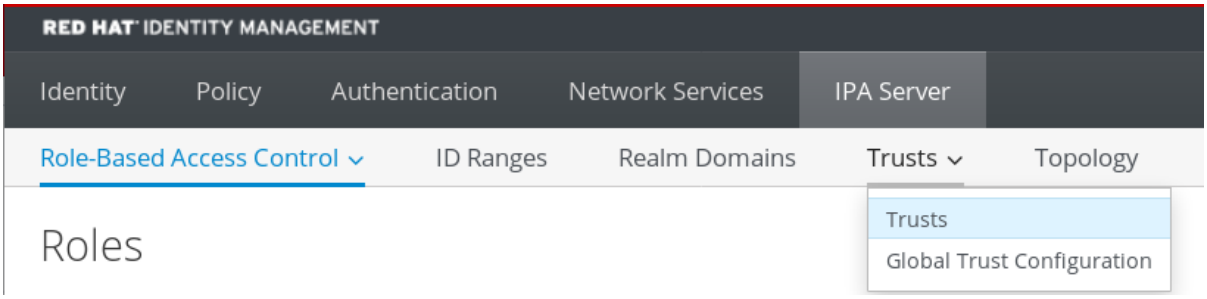
IdM 웹 UI를 사용하여 IdM 측에서 IdM(Identity Management)/Active Directory(AD) 신뢰 계약을 구성하려면 다음 절차를 따르십시오.

사전 요구 사항

- *DNS가 올바르게 구성되어 있습니다. IdM 및 AD 서버 모두 서로 이름을 확인할 수 있어야 합니다.*
- *지원되는 AD 및 IdM 버전이 배포됩니다.*
- *Kerberos 티켓을 받았습니다.*
- *웹 UI에 대한 신뢰를 생성하기 전에 다음에 설명된 대로 신뢰에 대해 IdM 서버를 준비합니다. 신뢰를 위한 IdM 서버 준비.*
- *IdM 관리자로 로그인해야 합니다.*

절차

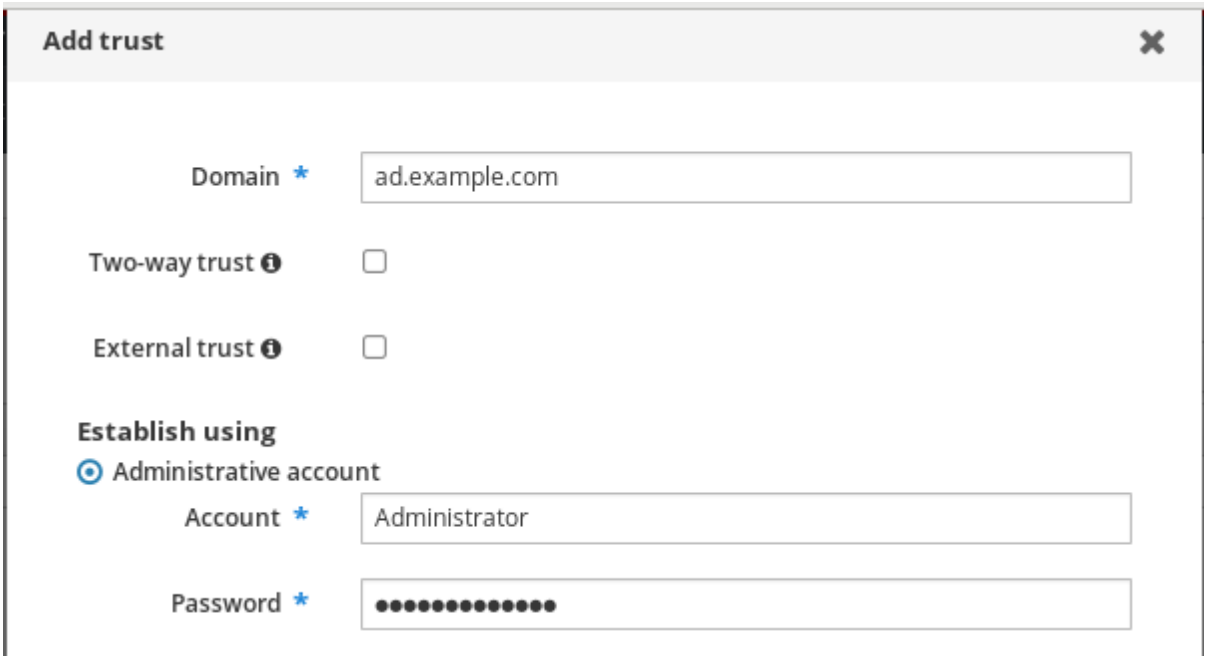
1. *관리자 권한으로 IdM 웹 UI에 로그인합니다. 자세한 내용은 웹 브라우저에서 IdM 웹 UI 액세스를 참조하십시오.*
2. *IdM 웹 UI에서* ***IPA 서버*** *탭을 클릭합니다.*
3. ***IPA 서버*** *탭에서 신뢰 탭을* ***클릭합니다****.*
4. *드롭다운 메뉴에서 신뢰 옵션을* ***선택합니다****.*



5. *Add(추가)* 단추를 클릭합니다.

6. ***신뢰 추가*** 대화 상자에서 Active Directory 도메인 이름을 입력합니다.

7. ***계정*** 및 ***암호*** 필드에 Active Directory 관리자의 관리자 자격 증명을 추가합니다.



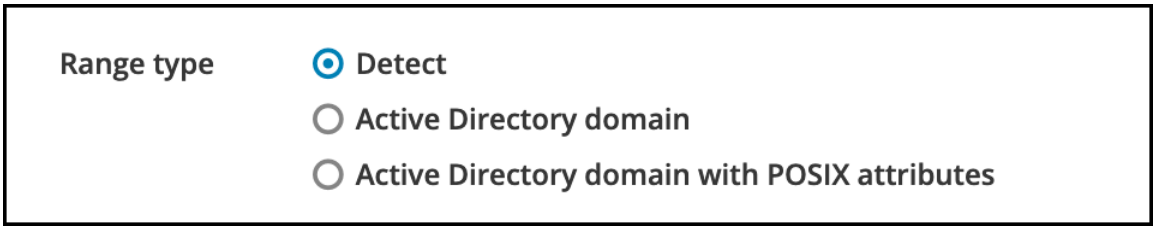
8. *(선택 사항) AD 사용자 및 그룹이 IdM의 리소스에 액세스할 수 있도록 하려면* ***양방향 트러스트*** *를 선택합니다. 그러나 IdM의 양방향 신뢰는 사용자에게 AD의 단방향 신뢰 솔루션에 비해 추가 권한을 부여하지 않습니다. 두 솔루션 모두 기본 크로스 포리스트 트러스트 필터링 설정으로 인해 동일하게 간주됩니다.*

9. *(선택 사항) AD 도메인의 루트 도메인이 아닌 트러스트를 구성하는* ***경우 외부*** *신뢰를 선택합니다. 포리스트 신뢰는 항상 IdM과 Active Directory 포리스트의 루트 도메인 간의 신뢰를 구축해야 하지만, AD 포리스트에 있는 모든 도메인에 대한 외부 트러스트를 IdM에서 모든 도메인으로 설정할 수 있습니다.*

10. *(선택 사항) 기본적으로 신뢰 설치 스크립트는 적절한 ID 범위 유형을 감지하려고 합니다. 다음 옵션 중 하나를 선택하여 ID 범위 유형을 명시적으로 설정할 수도 있습니다.*

    a. *SSSD가 해당 ECDHE를 기반으로 AD 사용자에 대한 UID 및 GID를 자동으로 생성하려면* ***Active Directory 도메인*** *ID 범위 유형을 선택합니다. 가장 일반적인 구성입니다.*

    b. *Active Directory에서 사용자의 POSIX 속성을 구성하고(예:* ***uidNumber*** *및* ***gidNumber****) SSSD에서 이 정보를 처리하려면* ***POSIX 속성 ID 범위 유형이 있는 Active Directory 도메인*** *을 선택합니다.*



주의

*기본 **Detect** 옵션에 **Range 유형** 설정을 남겨 두면 IdM에서 포리스트 루트 도메인의 AD 도메인 컨트롤러에서 세부 정보를 요청하여 적절한 범위 유형을 자동으로 선택합니다. IdM에서 POSIX 속성을 감지하지 않으면 신뢰 설치 스크립트에서 **Active Directory 도메인** ID 범위를 선택합니다.*

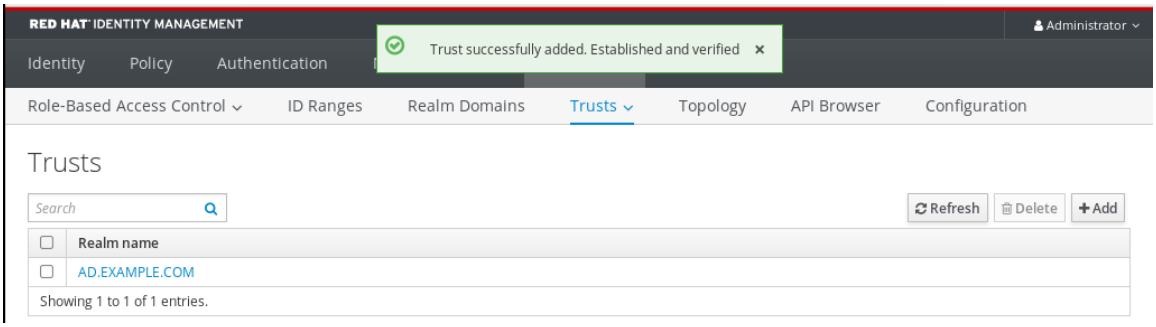
*IdM이 포리스트 루트 도메인에서 POSIX 속성을 감지하면 신뢰 설치 스크립트에서 **POSIX 속성 ID 범위가 있는 Active Directory 도메인** 을 선택하고 UID 및 GID가 AD에 올바르게 정의되어 있다고 가정합니다. AD에서 POSIX 속성이 올바르게 설정되지 않은 경우 AD 사용자를 확인할 수 없습니다.*

예를 들어, IdM 시스템에 대한 액세스가 필요한 사용자 및 그룹이 프리브릭 루트 도메인의 일부가 아닌 포리스트 도메인의 하위 도메인에 있는 경우 설치 스크립트에서 하위 AD 도메인에 정의된 POSIX 속성을 감지하지 못할 수 있습니다. 이 경우 신뢰를 설정할 때 POSIX ID 범위 유형을 명시적으로 선택하는 것이 좋습니다.

11. ***추가**를 클릭합니다.*

검증 단계

- *IdM 서버에 신뢰가 성공적으로 추가되면 IdM 웹 UI에 녹색 팝업 창이 표시됩니다. 이는 다음을 의미합니다.*
  - *도메인 이름 있음*
  - *Windows Server의 사용자 이름 및 암호가 올바르게 추가되었습니다.*



이제 신뢰 연결 및 Kerberos 인증을 계속 테스트할 수 있습니다.

9.4. ANSIBLE을 사용하여 신뢰 계약 설정

Ansible 플레이북을 사용하여 IdM(Identity Management)과 AD(Active Directory) 간에 단방향 신뢰 계약을 설정하려면 다음 절차를 따르십시오. 다음과 같은 세 가지 유형의 트러스트 계약을 구성할 수 있습니다.

- **One-way trust** expects. 단방향 신뢰로 인해 AD(Active Directory) 사용자 및 그룹이 IdM의 리소스에 액세스할 수 있지만 다른 방법은 액세스할 수 없습니다. IdM 도메인은 AD 포리스트를 신뢰하지만 AD 포리스트에서는 IdM 도메인을 신뢰하지 않습니다.

- **양방향 trust expect: Two-**way trust를 통해 AD 사용자 및 그룹이 IdM의 리소스에 액세스할 수 있습니다.
  S4U2Self 및 S4U2 Proxy Microsoft 확장에서 신뢰할 수 있는 경계를 통해 작동하도록 Microsoft SQL Server와 같은 솔루션에 대한 양방향 신뢰를 구성해야 합니다. RHEL IdM 호스트의 애플리케이션은 AD 사용자에 대한 Active Directory 도메인 컨트롤러에서 **S4U2Self 또는 S4U2Proxy** 정보를 요청할 수 있으며 양방향 신뢰에서는 이 기능을 제공합니다.

  이 양방향 신뢰 기능은 IdM 사용자가 Windows 시스템에 로그인할 수 없으며 IdM의 양방향 신뢰는 사용자에게 AD의 단방향 신뢰 솔루션에 비해 추가 권한을 부여하지 않습니다.

  - 양방향 신뢰를 생성하려면 아래 플레이북 작업에 다음 변수를 추가합니다. **two_way: true**

- **외부 신뢰** - 다른 포리스트의 IdM과 AD 도메인 간의 신뢰 관계입니다. 포리스트 신뢰는 항상 IdM과 Active Directory 포리스트의 루트 도메인 간 신뢰를 구축해야 하지만 외부 신뢰는 IdM에서 포리스트 내 도메인으로 외부 트러스트를 설정할 수 있습니다. 이는 관리 또는 조직의 이유로 인해 포리스트 루트 도메인 간에 포리스트의 신뢰를 설정할 수 없는 경우에만 권장됩니다.

  - 외부 신뢰를 생성하려면 아래 플레이북 작업에 다음 변수를 추가합니다. **external: true**

사전 요구 사항

- Windows 관리자의 사용자 이름 및 암호입니다.
- IdM **관리자** 암호입니다.
- 신뢰를 위해 IdM 서버를 준비했습니다.
- 4.8.7 버전의 IdM을 사용하고 있습니다. 서버에 설치한 IdM 버전을 보려면 **ipa --version** 를 실행합니다.
- 다음 요구 사항을 충족하도록 Ansible 제어 노드를 구성했습니다.
  - Ansible 버전 2.14 이상을 사용하고 있습니다.
  - Ansible 컨트롤러에 **ansible-freeipa** 패키지가 설치되어 있습니다.
  - 이 예제에서는 **~/MyPlaybook/** 디렉터리에서 IdM 서버의 정규화된 도메인 이름(FQDN)을 사용하여 Ansible 인벤토리 파일을 생성했다고 가정합니다.
  - 이 예제에서는 **secret.yml** Ansible 자격 증명 모음이 **ipaadmin_password** 를 저장하는 것으로 가정합니다.
- **ansible-freeipa** 모듈이 실행되는 노드인 대상 노드는 IdM 도메인의 일부인 IdM 클라이언트, 서버 또는 복제본입니다.

절차

1. **~/MyPlaybooks/** 디렉터리로 이동합니다.

```
$ cd ~/MyPlaybooks/
```

2. *사용 사례에 따라 다음 시나리오 중 하나를 선택합니다.*

   - *ID 매핑 신뢰 계약을 생성하려면 SSSD에서 libc를 기반으로 AD 사용자 및 그룹의 UID 및 GID를 자동으로 생성하는 경우 다음 콘텐츠를 사용하여 **add-trust.yml** 플레이북을 생성합니다.*

     ```
     ---
     - name: Playbook to create a trust
       hosts: ipaserver

       vars_files:
       - /home/user_name/MyPlaybooks/secret.yml
       tasks:
         - name: ensure the trust is present
           ipatrust:
             ipaadmin_password: "{{ ipaadmin_password }}"
             realm: ad.example.com
             admin: Administrator
             password: secret_password
             range_type: ipa-ad-trust
             state: present
     ```

     에에서는 다음을 수행합니다.

     - ***realm** 은 AD 영역 이름 문자열을 정의합니다.*
     - ***admin** 은 AD 도메인 관리자 문자열을 정의합니다.*
     - ***password** 는 AD 도메인 관리자의 암호 문자열을 정의합니다.*

   - *POSIX 신뢰 계약을 만들려면 SSSD에서 AD에 저장된 POSIX 속성(예: **uidNumber** 및 **gidNumber**)을 처리하는 경우 다음 콘텐츠를 사용하여 **add-trust.yml** 플레이북을 만듭니다.*

     ```
     ---
     - name: Playbook to create a trust
       hosts: ipaserver

       vars_files:
       - /home/user_name/MyPlaybooks/secret.yml
       tasks:
         - name: ensure the trust is present
           ipatrust:
             ipaadmin_password: "{{ ipaadmin_password }}"
             realm: ad.example.com
             admin: Administrator
             password: secret_password
             range_type: ipa-ad-trust-posix
             state: present
     ```

   - *VirtIO 루트 도메인의 AD 도메인 컨트롤러에서 다음 콘텐츠를 사용하여 세부 정보를 요청하여 IdM에서 적절한 범위 유형, **ipa-ad-trust** 또는 **ipa-ad-trust-posix** 를 자동으로 선택하려는 신뢰 계약을 생성하려면 다음 콘텐츠를 사용하여 **add-trust.yml** 플레이북을 생성합니다.*

     ```
     ---
     - name: Playbook to create a trust
       hosts: ipaserver
     ```

```
vars_files:
- /home/user_name/MyPlaybooks/secret.yml
tasks:
  - name: ensure the trust is present
    ipatrust:
      ipaadmin_password: "{{ ipaadmin_password }}"
      realm: ad.example.com
      admin: Administrator
      password: secret_password
      state: present
```

주의

*신뢰를 생성할 때 ID 범위 유형을 지정하지 않고 IdM에서 AD forest 루트 도메인의 POSIX 속성을 검색하지 않으면 신뢰 설치 스크립트에서 **Active Directory 도메인** ID 범위를 선택합니다.*

*IdM이 포리스트 루트 도메인에서 POSIX 속성을 감지하면 신뢰 설치 스크립트에서 **POSIX 속성 ID 범위가 있는 Active Directory 도메인** 을 선택하고 UID 및 GID가 AD에 올바르게 정의되어 있다고 가정합니다.*

그러나 POSIX 속성이 AD에서 올바르게 설정되지 않으면 AD 사용자를 확인할 수 없습니다. 예를 들어, IdM 시스템에 대한 액세스가 필요한 사용자 및 그룹이 프리브릭 루트 도메인의 일부가 아닌 포리스트 도메인의 하위 도메인에 있는 경우 설치 스크립트에서 하위 AD 도메인에 정의된 POSIX 속성을 감지하지 못할 수 있습니다. 이 경우 신뢰를 설정할 때 POSIX ID 범위 유형을 명시적으로 선택하는 것이 좋습니다.

3. *파일을 저장합니다.*

4. *Ansible 플레이북을 실행합니다. Playbook 파일, **secret.yml** 파일을 보호하는 암호를 저장하는 파일, 인벤토리 파일을 지정합니다.*

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory add-trust.yml
```

추가 리소스

- */usr/share/doc/ansible-freeipa/README-trust.md*
- */usr/share/doc/ansible-freeipa/playbooks/trust*

9.5. KERBEROS 구성 확인

Kerberos 구성을 확인하려면 IdM(Identity Management) 사용자의 티켓을 받을 수 있는지 테스트하고 IdM 사용자가 서비스 티켓을 요청할 수 있는지 테스트합니다.

절차

1. *AD(Active Directory) 사용자의 티켓을 요청하십시오.*

-

```
[root@ipaserver ~]# kinit user@AD.EXAMPLE.COM
```

2. IdM 도메인 내의 서비스에 대한 서비스 티켓을 요청하십시오.

```
[root@server ~]# kvno -S host server.idm.example.com
```

AD 서비스 티켓이 성공적으로 승인되면 요청된 다른 모든 티켓과 함께 TGT(Cross-realm ticket-granting ticket)가 표시됩니다. TGT의 이름은ECDHEtECDHE/IPA.DOMAIN@AD.DOMAIN입니다.

```
[root@server ]# klist
Ticket cache: KEYRING:persistent:0:krb_ccache_hRtox00
Default principal: user@AD.EXAMPLE.COM

Valid starting       Expires              Service principal
03.05.2016 18:31:06  04.05.2016 04:31:01  host/server.idm.example.com@IDM.EXAMPLE.COM
 renew until 04.05.2016 18:31:00
03.05.2016 18:31:06 04.05.2016 04:31:01 krbtgt/IDM.EXAMPLE.COM@AD.EXAMPLE.COM
 renew until 04.05.2016 18:31:00
03.05.2016 18:31:01  04.05.2016 04:31:01  krbtgt/AD.EXAMPLE.COM@AD.EXAMPLE.COM
 renew until 04.05.2016 18:31:00
```

localauth 플러그인은 Kerberos 사용자를 SSSD(Local System Security Services Daemon) 사용자 이름에 매핑합니다. 이를 통해 AD 사용자는 Kerberos 인증을 사용하고 Linux 서비스에 액세스하여 GSSAPI 인증을 직접 지원할 수 있습니다.

9.6. IDM에서 신뢰 구성 확인

신뢰를 구성하기 전에 IdM(Identity Management) 및 AD(Active Directory) 서버가 서로 확인할 수 있는지 확인합니다.

사전 요구 사항

- 관리자 권한으로 로그인해야 합니다.

절차

1. UDP를 통한 MS DC Kerberos 및 TCP 서비스 레코드를 통해 LDAP에 대한 DNS 쿼리를 실행합니다.

```
[root@server ~]# dig +short -t SRV _kerberos._udp.dc._msdcs.idm.example.com.
0 100 88 server.idm.example.com.

[root@server ~]# dig +short -t SRV _ldap._tcp.dc._msdcs.idm.example.com.
0 100 389 server.idm.example.com.
```

이 명령을 수행하면 **ipa-adtrust-install** 이 실행된 모든 IdM 서버가 나열됩니다. 일반적으로 첫 번째 신뢰 관계를 설정하기 전에 **ipa-adtrust-install** 이 IdM 서버에서 실행되지 않은 경우 출력이 비어 있습니다.

2. TCP 서비스 레코드를 통해 Kerberos 및 LDAP에 대한 DNS 쿼리를 실행하여 IdM이 AD의 서비스 레코드를 확인할 수 있는지 확인합니다.

```
[root@server ~]# dig +short -t SRV _kerberos._tcp.dc._msdcs.ad.example.com.
0 100 88 addc1.ad.example.com.
```

```
[root@ipaserver ~]# dig +short -t SRV _ldap._tcp.dc._msdcs.ad.example.com.
0 100 389 addc1.ad.example.com.
```

.

9.7. AD 에서 신뢰 구성 확인

신뢰를 구성한 후 다음을 확인합니다.

- IdM(Identity Management) 호스팅 서비스는 AD(Active Directory) 서버에서 확인할 수 있습니다.
- AD 서비스는 AD 서버에서 확인할 수 있습니다.

사전 요구 사항

- 관리자 권한으로 로그인해야 합니다.

절차

1. AD 서버에서 서비스 레코드를 조회하도록 **nslookup.exe** 유틸리티를 설정합니다.

```
C:\>nslookup.exe
> set type=SRV
```

2. UDP를 통한 Kerberos의 도메인 이름과 TCP 서비스 레코드를 통한 LDAP를 입력합니다.

```
> _kerberos._udp.idm.example.com.
_kerberos._udp.idm.example.com.       SRV service location:
    priority             = 0
    weight               = 100
    port                 = 88
    svr hostname   = server.idm.example.com
> _ldap._tcp.idm.example.com
_ldap._tcp.idm.example.com       SRV service location:
    priority             = 0
    weight               = 100
    port                 = 389
    svr hostname   = server.idm.example.com
```

3. 서비스 유형을 TXT로 변경하고 IdM Kerberos 영역 이름을 사용하여 TXT 레코드에 대한 DNS 쿼리를 실행합니다.

```
C:\>nslookup.exe
> set type=TXT
> _kerberos.idm.example.com.
_kerberos.idm.example.com.       text =

    "IDM.EXAMPLE.COM"
```

4. UDP를 통한 MS DC Kerberos 및 TCP 서비스 레코드를 통해 LDAP에 대한 DNS 쿼리를 실행합니다.

```
C:\>nslookup.exe
```

```
> set type=SRV
> _kerberos._udp.dc._msdcs.idm.example.com.
_kerberos._udp.dc._msdcs.idm.example.com.       SRV service location:
    priority = 0
    weight = 100
    port = 88
    svr hostname = server.idm.example.com
> _ldap._tcp.dc._msdcs.idm.example.com.
_ldap._tcp.dc._msdcs.idm.example.com.       SRV service location:
    priority = 0
    weight = 100
    port = 389
    svr hostname = server.idm.example.com
```

Active Directory에서는 다른 AD 도메인 컨트롤러 및 IdM 신뢰 컨트롤러와 같은 AD별 프로토콜 요청에 응답할 수 있는 도메인 컨트롤러만 검색해야 합니다. ***ipa-adtrust-install*** *툴을 사용하여 IdM 서버를 신뢰 컨트롤러로 승격하고* ***ipa server-role-find --role 'AD trust controller' 명령을 사용하여 어떤 서버가*** *신뢰 컨트롤러인지 확인할 수 있습니다.*

5. *AD 서버에서 AD 서비스를 확인할 수 있는지 확인합니다.*

```
C:\>nslookup.exe
> set type=SRV
```

6. *UDP를 통한 Kerberos의 도메인 이름과 TCP 서비스 레코드를 통한 LDAP를 입력합니다.*

```
> _kerberos._udp.dc._msdcs.ad.example.com.
_kerberos._udp.dc._msdcs.ad.example.com.  SRV service location:
    priority = 0
    weight = 100
    port = 88
    svr hostname = addc1.ad.example.com
> _ldap._tcp.dc._msdcs.ad.example.com.
_ldap._tcp.dc._msdcs.ad.example.com.  SRV service location:
    priority = 0
    weight = 100
    port = 389
    svr hostname = addc1.ad.example.com
```

9.8. 신뢰 에이전트 생성

신뢰 에이전트는 AD 도메인 컨트롤러에 대해 ID 조회를 수행할 수 있는 IdM 서버입니다.

예를 들어 Active Directory에 대한 신뢰가 있는 IdM 서버의 복제본을 생성하는 경우 복제본을 신뢰 에이전트로 설정할 수 있습니다. 복제본에 AD 신뢰 에이전트 역할이 자동으로 설치되지 않습니다.

사전 요구 사항

- *IdM은 Active Directory 신뢰와 함께 설치됩니다.*
- ***sssd-tools*** *패키지가 설치됩니다.*

절차

1. 기존 신뢰 컨트롤러에서 **ipa-adtrust-install --add-agents** 명령을 실행합니다.

```
[root@existing_trust_controller]# ipa-adtrust-install --add-agents
```

명령은 대화식 구성 세션을 시작하고 에이전트를 설정하는 데 필요한 정보를 입력하라는 메시지를 표시합니다.

2. 신뢰 에이전트에서 IdM 서비스를 다시 시작합니다.

```
[root@new_trust_agent]# ipactl restart
```

3. 신뢰 에이전트의 SSSD 캐시에서 모든 항목을 제거합니다.

```
[root@new_trust_agent]# sssctl cache-remove
```

4. 복제본에 AD 신뢰 에이전트 역할이 설치되었는지 확인합니다.

```
[root@existing_trust_controller]# ipa server-show new_replica.idm.example.com
...
Enabled server roles: CA server, NTP server, AD trust agent
```

추가 리소스

- **--add-agents** 옵션에 대한 자세한 내용은 **ipa-adtrust-install(1)** 매뉴얼 페이지를 참조하십시오.
- 신뢰 에이전트에 대한 자세한 내용은 계획 ID 관리 가이드의 컨트롤러 및 신뢰 에이전트 신뢰를 참조하십시오.

9.9. CLI에서 POSIX ID 범위에 대한 자동 개인 그룹 매핑 활성화

기본적으로 SSSD는 AD에 저장된 POSIX 데이터에 의존하는 POSIX 트러스트를 설정한 경우 AD(Active Directory) 사용자에 대해 개인 그룹을 매핑하지 않습니다. AD 사용자에게 기본 그룹이 구성되지 않은 경우 IdM은 이를 확인할 수 없습니다.

다음 절차에서는 명령줄에서 **auto_private_groups** SSSD 매개 변수에 대한 **하이브리드** 옵션을 설정하여 ID 범위에 대해 자동 개인 그룹 매핑을 활성화하는 방법을 설명합니다. 결과적으로 IdM은 AD에 기본 그룹이 구성되지 않은 AD 사용자를 확인할 수 있습니다.

사전 요구 사항

- IdM과 AD 환경 간에 POSIX 크로스 포리스트 신뢰가 성공적으로 설정되었습니다.

절차

1. 모든 ID 범위를 표시하고 수정할 AD ID 범위를 기록해 둡니다.

```
[root@server ~]# ipa idrange-find
----------------
2 ranges matched
----------------
  Range name: IDM.EXAMPLE.COM_id_range
  First Posix ID of the range: 882200000
  Number of IDs in the range: 200000
```

```
Range type: local domain range

Range name: AD.EXAMPLE.COM_id_range
First Posix ID of the range: 1337000000
Number of IDs in the range: 200000
Domain SID of the trusted domain: S-1-5-21-4123312420-990666102-3578675309
Range type: Active Directory trust range with POSIX attributes
----------------------------
Number of entries returned 2
----------------------------
```

2. **ipa idrange-mod** 명령을 사용하여 AD ID 범위의 자동 개인 그룹 동작을 조정합니다.

```
[root@server ~]# ipa idrange-mod --auto-private-groups=hybrid
AD.EXAMPLE.COM_id_range
```

3. 새 설정을 활성화하려면 SSSD 캐시를 재설정합니다.

```
[root@server ~]# sss_cache -E
```

추가 리소스

- AD 사용자의 프라이빗 그룹을 자동으로 매핑하는 옵션

9.10. IDM WEBUI에서 POSIX ID 범위의 자동 개인 그룹 매핑 활성화

기본적으로 SSSD는 AD에 저장된 POSIX 데이터에 의존하는 POSIX 트러스트를 설정한 경우 AD(Active Directory) 사용자에 대해 개인 그룹을 매핑하지 않습니다. AD 사용자에게 기본 그룹이 구성되지 않은 경우 IdM은 이를 확인할 수 없습니다.

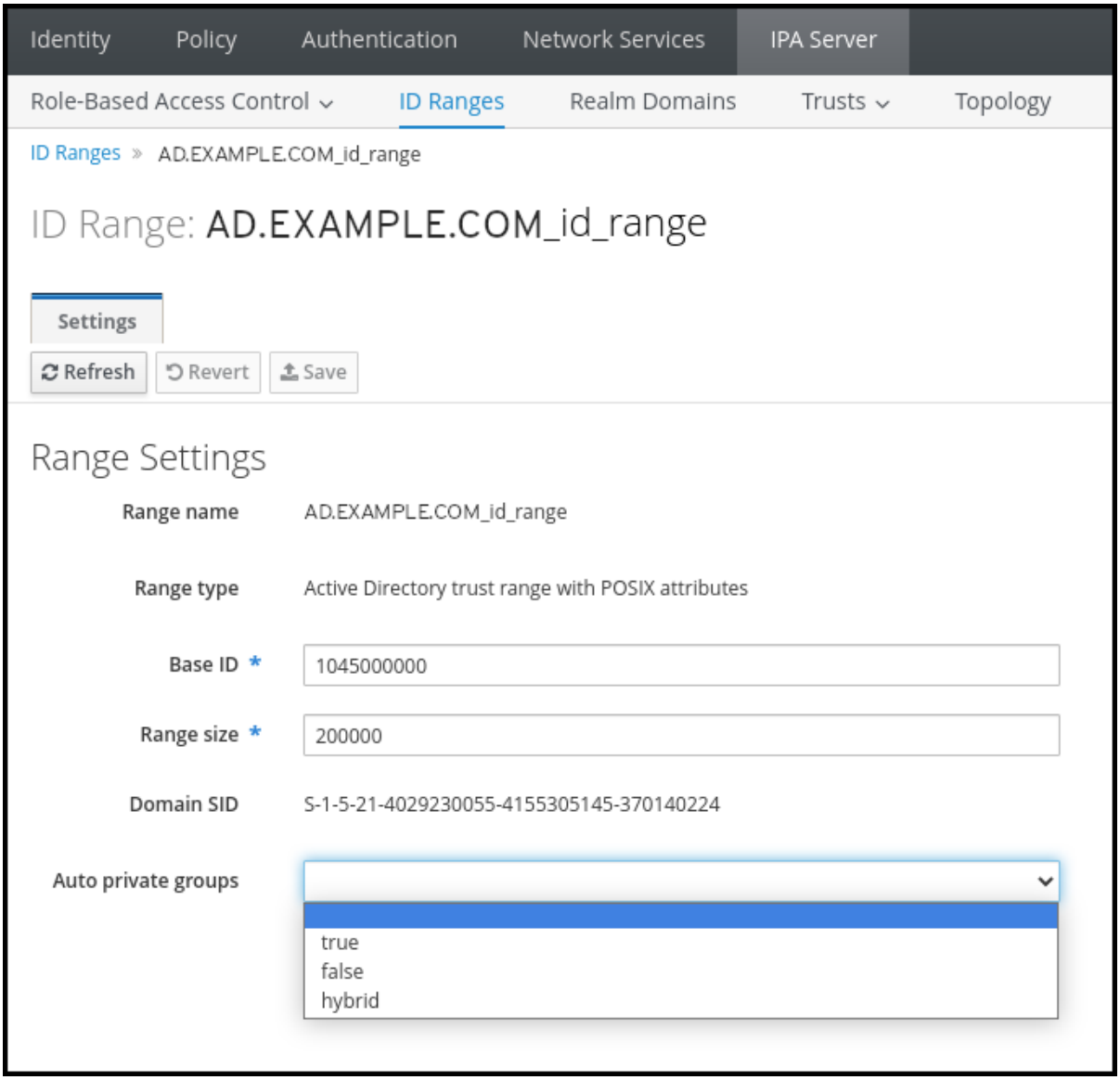
다음 절차에서는 IdM(Identity Management) WebUI에서 **auto_private_groups** SSSD 매개변수에 대한 **하이브리드** 옵션을 설정하여 ID 범위에 대해 자동 개인 그룹 매핑을 활성화하는 방법을 설명합니다. 결과적으로 IdM은 AD에 기본 그룹이 구성되지 않은 AD 사용자를 확인할 수 있습니다.

사전 요구 사항

- IdM과 AD 환경 간에 POSIX 크로스 포리스트 신뢰가 성공적으로 설정되었습니다.

절차

1. 사용자 이름과 암호를 사용하여 IdM 웹 UI에 로그인합니다.
2. **IPA 서버 → ID 범위** 탭을 엽니다.
3. 변경할 ID 범위를 선택합니다(예: **AD.EXAMPLE.COM_id_range**).
4. **Auto private groups** 드롭다운 메뉴에서 **하이브리드** 옵션을 선택합니다.



5. ***저장*** *버튼을 클릭하여 변경 사항을 저장합니다.*

추가 리소스

- *AD 사용자의 프라이빗 그룹을 자동으로 매핑하는 옵션*

10장. 가장 신뢰할 수 있는 교차 신뢰 설정 문제 해결

IdM(Identity Management) 환경과 AD(Active Directory) 포리스트 간의 교차 포리스트 신뢰를 구성하는 프로세스 문제 해결에 대해 자세히 알아보십시오.

10.1. AD로 상호 간 트러스트를 설정할 때 이벤트 시퀀스

ipa trust-add 명령을 사용하여 AD(Active Directory) 도메인 컨트롤러(DC)와의 상호 간 트러스트를 설정하는 경우 명령은 명령을 실행한 사용자를 대신하여 작동하며 IdM 서버에서 다음 작업을 수행합니다. 가장 간결한 신뢰를 설정하는 데 문제가 있는 경우 이 목록을 사용하여 문제를 좁히고 문제를 해결할 수 있습니다.

다음 단계: 명령은 설정 및 입력 확인

1. IdM 서버에 **신뢰 컨트롤러** 역할이 있는지 확인합니다.
2. **ipa trust-add** 명령에 전달된 옵션을 확인합니다.
3. 신뢰할 수 있는est 루트 도메인과 연관된 ID 범위를 검증합니다. ID 범위 유형 및 속성을 **ipa trust-add** 명령에 대한 옵션으로 지정하지 않은 경우 Active Directory에서 검색됩니다.

2부: 이 명령은 Active Directory 도메인에 대한 신뢰를 설정하려고 합니다.

4. 각 신뢰 방향에 대해 별도의 신뢰 개체를 만듭니다. 각 오브젝트는 양쪽(IdM 및 AD)에서 생성됩니다. 단방향 트러스트를 설정하는 경우 각 측에 하나의 개체만 생성됩니다.
5. IdM 서버는 Samba 제품군을 사용하여 Active Directory용 도메인 컨트롤러 기능을 처리하고 대상 AD PDC에서 신뢰 개체를 생성합니다.
    a. IdM 서버는 대상 DC의 **IPC$** 공유에 대한 보안 연결을 설정합니다. RHEL 8.4부터 연결에는 적어도 Windows Server 2012 이상의 SMB3 프로토콜이 있어야 세션에 사용된 AES 기반 암호화를 통해 연결이 충분히 보호되도록 합니다.
    b. IdM 서버 쿼리는 **LSA QueryTrustedDomainInfoByName** 호출을 사용하여 신뢰할 수 있는 도메인 오브젝트(TDO)의 존재 여부를 쿼리합니다.
    c. TDO가 이미 있는 경우 **LSA DeleteTrustedDomain** 호출을 사용하여 제거합니다.

참고

이 호출은 트러스트를 설정하는 데 사용된 AD 사용자 계정에 **Incoming Forest Trust Builders** 그룹 멤버와 같은 forest 루트에 대한 전체 **엔터프라이즈 관리자(EA) 또는 DDA(Domain Admin)** 권한이 없는 경우 실패합니다. 이전 TDO가 자동으로 제거되지 않으면 AD 관리자가 AD에서 수동으로 제거해야 합니다.

    d. IdM 서버는 **LSA CreateTrustedDomainEx2** 호출을 사용하여 새 TDO를 생성합니다. TDO 자격 증명은 128개의 임의 문자가 있는 Samba 제공 암호 생성기를 사용하여 무작위로 생성됩니다.
    e. 그런 다음 새 TDO가 **LSA SetInformationTrustedDomain** 호출을 통해 수정되어 신뢰에서 지원하는 암호화 유형이 올바르게 설정됩니다.
        i. Active Directory 설계 방식으로 인해 **RC4_HMAC_md5** 암호화 유형이 사용 중인 RC4 키가 없는 경우에도 사용할 수 있습니다.

ii. ***AES128_CTS_HMAC_SHA1_96*** *및* ***AES256_CTS_HMAC_SHA1_96*** *암호화 유형이 활성화되어 있습니다.*

참고

기본적으로 RHEL 9는 AD에 필요한 알고리즘인 SHA-1 암호화를 허용하지 않습니다. ***AD-SUPPORT*** *시스템 전체 암호화 하위 정책을 활성화하여 RHEL 9 IdM 서버에서 AD 도메인 컨트롤러와의 SHA-1 암호화를 허용하도록 설정해야 합니다. <link TBA>를 참조하십시오.*

6. *For a forest trust, verify that in-forest domains can be reachedly with an* ***LSA SetInformationTrustedDomain*** *call.*

7. ***LSA RSetForestTrustInformation*** *호출을 사용하여 IdM과 통신할 때 AD와의 통신이 가능한 경우 다른 포리스트(IdM)에 대한 신뢰 토폴로지 정보를 추가합니다.*

참고

이 단계는 다음 세 가지 이유 중 하나로 인해 충돌을 일으킬 수 있습니다.

1. *SID 네임스페이스 충돌은* ***LSA_SID_DISABLED_CONFLICT*** *오류로 보고됩니다. 이 충돌을 해결할 수 없습니다.*
2. *OPENSHIFT 네임스페이스 충돌은* ***LSA_NB_DISABLED_CONFLICT*** *오류로 보고됩니다. 이 충돌을 해결할 수 없습니다.*
3. *DNS 네임스페이스가* ***LSA_TLN_DISABLED_CONFLICT*** *오류로 보고되는 TLN(최상 수준 이름)과 충돌합니다. IdM 서버는 TLN 충돌을 자동으로 해결할 수 있습니다.*

TLN 충돌을 해결하기 위해 IdM 서버는 다음 단계를 수행합니다.

1. *충돌하는 포리스트에 대한est 신뢰 정보를 검색합니다.*
2. *IdM DNS 네임스페이스의 제외 항목을 AD forest에 추가합니다.*
3. *우리가 충돌하는 숲에 대한 도메인 신뢰 정보를 설정합니다.*
4. *이 경우, 신뢰를 원래의 숲으로 다시 형성하는 것입니다.*

IdM 서버는est 트러스트를 변경할 수 있는 AD 관리자 권한으로 ***ipa trust-add*** *명령을 인증한 경우에만 이러한 충돌을 해결할 수 있습니다. 이러한 권한에 액세스할 수 없는 경우 원래의 Specest 관리자는 Windows UI의* ***Active Directory Domains 및 Trusts*** *섹션에서 위의 단계를 수동으로 수행해야 합니다.*

8. *없는 경우 신뢰할 수 있는 도메인의 ID 범위를 만듭니다.*

9. *est 트러스트의 경우est 루트에서 Active Directory 도메인 컨트롤러를 쿼리하여 forest 토폴로지에 대한 자세한 내용을 확인합니다.For a forest trust, query Active Directory domain controllers from the forest root for details about the forest topology. IdM 서버는 이 정보를 사용하여 신뢰할 수 있는 포리스트의 추가 도메인에 대한 추가 ID 범위를 생성합니다.*

추가 리소스

- *신뢰 컨트롤러 및 신뢰 에이전트*

- *개요 문서 (Microsoft)*
- *기술 문서 (Microsoft)*
- *Active Directory의 권한 있는 계정 및 그룹 (Microsoft)*

10.2. AD 트러스트를 설정하기 위한 사전 요구 사항 체크리스트

다음 체크리스트를 사용하여 AD 도메인과의 신뢰 생성을 위한 사전 요구 사항을 검토할 수 있습니다.

표 10.1. 테이블

구성 요소	설정	추가 세부 정보
제품 버전	Active Directory 도메인이 지원되는 Windows Server 버전을 사용하고 있습니다.	지원되는 Windows Server 버전
AD Administrator 권한	Active Directory 관리 계정은 다음 그룹 중 하나의 구성원이어야 합니다. • AD forest의 **엔터프라이즈 관리자 (EA)** 그룹 • AD forest에 대한 **Domain Admins(DA)** 그룹est root domain for your AD forest	
네트워킹	모든 IdM 서버에 대해 Linux 커널에서 IPv6 지원이 활성화됩니다.	IdM의 IPv6 요구 사항
날짜 및 시간	두 서버의 날짜 및 시간 설정이 일치했는지 확인합니다.	IdM 시간 서비스 요구 사항

구성 요소	설정	추가 세부 정보
암호화 유형	다음 AD 계정에는 AES 암호화 키가 있습니다. ● AD 관리자 ● AD 사용자 계정 ● AD 서비스 최근 AD에서 AES 암호화를 활성화한 경우 다음 단계를 사용하여 새 AES 키를 생성합니다. 1. 포리스트의 모든 AD 도메인 간 신뢰 관계를 다시 구축할 수 있습니다. 2. AD Administrator, 사용자 계정 및 서비스의 암호를 변경합니다.	● IdM의 암호화 유형 지원 ● GPO를 사용하여 Active Directory의 AES 암호화 유형 활성화
방화벽	양방향 통신을 위해 IdM 서버 및 AD 도메인 컨트롤러에서 필요한 모든 포트를 열었습니다.	IdM과 AD 간 통신에 필요한 포트
DNS	● IdM과 AD에는 각각 고유한 기본 DNS 도메인이 있습니다. ● IdM 및 AD DNS 도메인이 겹치지 않습니다. ● LDAP 및 Kerberos 서비스의 적절한 DNS 서비스 (SRV) 레코드 ● 신뢰의 모든 DNS 도메인에서 DNS 레코드를 확인할 수 있습니다. ● Kerberos 영역 이름은 기본 DNS 도메인 이름의 대문자 버전입니다. 예를 들어 DNS 도메인 **example.com** 에는 해당 Kerberos 영역 **EXAMPLE.COM**이 있습니다.	신뢰에 대한 DNS 및 영역 설정 구성
토폴로지	구성한 IdM 서버를 신뢰 컨트롤러로 설정하려고 합니다.	신뢰 컨트롤러 및 신뢰 에이전트

10.3. AD 신뢰 설정 시도의 디버그 로그 수집

IdM 환경과 AD 도메인 간에 신뢰를 설정하는 데 문제가 발생하는 경우 다음 단계를 사용하여 자세한 오류 로깅을 활성화하여 신뢰 시도 로그를 수집할 수 있습니다. 이러한 로그를 검토하여 문제 해결에 도움이 되는 로그를 확인하거나 Red Hat 기술 지원 케이스에서 해당 로그를 제공할 수 있습니다.

사전 요구 사항

- *IdM 서비스를 다시 시작하려면 root 권한이 필요합니다.*

절차

1. *IdM 서버에 대한 디버깅을 활성화하려면 다음 콘텐츠를 사용하여* ***/etc/ipa/server.conf*** *파일을 생성하십시오.*

```
[global]
debug=True
```

2. ***httpd*** *서비스를 다시 시작하여 디버깅 구성을 로드합니다.*

```
[root@trust_controller ~]# systemctl restart httpd
```

3. ***smb*** *및* ***winbind*** *서비스를 중지합니다.*

```
[root@trust_controller ~]# systemctl stop smb winbind
```

4. ***smb*** *및* ***winbind*** *서비스의 디버깅 로그 수준을 설정합니다.*

```
[root@trust_controller ~]# net conf setparm global 'log level' 100
```

5. *IdM 프레임워크에서 사용하는 Samba 클라이언트 코드에 대한 디버그 로깅을 활성화하려면* ***/usr/share/ipa/smb.conf.empty*** *구성 파일을 편집하여 다음 내용을 보유합니다.*

```
[global]
log level = 100
```

6. *이전 Samba 로그를 제거합니다.*

```
[root@trust_controller ~]# rm /var/log/samba/log.*
```

7. ***smb*** *및* ***winbind*** *서비스를 시작합니다.*

```
[root@trust_controller ~]# systemctl start smb winbind
```

8. *자세한 정보 표시 모드가 활성화된 트러스트를 설정하려고 할 때 타임스탬프를 출력합니다.*

```
[root@trust_controller ~]# date; ipa -vvv trust-add --type=ad ad.example.com
```

9. *실패한 요청에 대한 정보는 다음 오류 로그 파일을 확인하십시오.*

   a. ***/var/log/httpd/error_log***

   b. ***/var/log/samba/log.****

10. *디버깅을 비활성화합니다.*

```
[root@trust_controller ~]# mv /etc/ipa/server.conf /etc/ipa/server.conf.backup
[root@trust_controller ~]# systemctl restart httpd
[root@trust_controller ~]# systemctl stop smb winbind
[root@trust_controller ~]# net conf setparm global 'log level' 0
[root@trust_controller ~]# mv /usr/share/ipa/smb.conf.empty
/usr/share/ipa/smb.conf.empty.backup
[root@trust_controller ~]# systemctl start smb winbind
```

11. *(선택 사항) 인증 문제의 원인을 확인할 수 없는 경우:*

    a. *최근에 생성된 로그 파일을 수집하고 보관합니다.*

    ```
    [root@trust_controller ~]# tar -cvf debugging-trust.tar /var/log/httpd/error_log
    /var/log/samba/log.*
    ```

    b. *Red Hat 기술 지원 케이스를 열고 시도 후 타임 스탬프 및 디버그 로그를 제공합니다.*

추가 리소스

- *IPA - AD 트러스트 문제 해결*

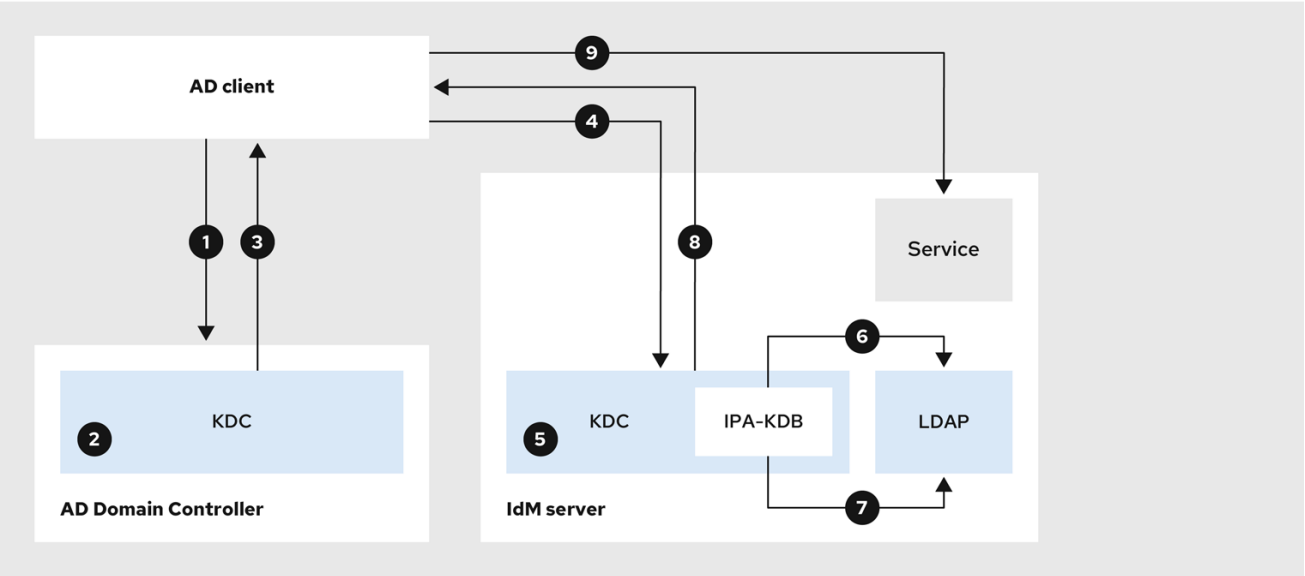
11장. 다른 포리스트의 서비스에 대한 클라이언트 액세스 문제 해결

IdM(Identity Management)과 AD(Active Directory) 환경 간에 신뢰를 구성한 후 한 도메인의 클라이언트가 다른 도메인의 서비스에 액세스할 수 없는 문제가 발생할 수 있습니다. 다음 다이어그램을 사용하여 문제를 해결합니다.

11.1. AD FOREST 루트 도메인의 호스트가 IDM 서버에서 서비스를 요청할 때 정보 흐름

다음 다이어그램에서는 Active Directory(AD) 클라이언트가 IdM(Identity Management) 도메인에서 서비스를 요청할 때 정보 흐름을 설명합니다.

AD 클라이언트에서 IdM 서비스에 액세스하는 데 문제가 있는 경우 이 정보를 사용하여 문제 해결 노력을 좁히고 문제 소스를 확인할 수 있습니다.



231_RHEL_0422

1. AD 클라이언트는 ADDC(Kerberos Distribution Center)에 연결하여 IdM 도메인에서 서비스에 대한 TGS 요청을 수행합니다.
2. AD EgressIP은 서비스가 신뢰할 수 있는 IdM 도메인에 속하는지 인식합니다.
3. AD EgressIP은 클라이언트에 신뢰할 수 있는 IdM key에 대한 참조와 함께 TGT(cross-realm ticket-granting ticket)를 클라이언트에 보냅니다.
4. AD 클라이언트는 cross-realm TGT를 사용하여 IdM EgressIP에 티켓을 요청합니다.
5. IdM EgressIP은 교차 실제 TGT와 함께 전송된 Privileged Attribute Certificate (MS-PAC)의 유효성을 검사합니다.
6. IPA-KDB 플러그인은 LDAP 디렉토리를 확인하여 요청된 서비스에 대한 티켓을 받을 수 있는 외부 주체가 허용되는지 확인할 수 있습니다.
7. IPA-KDB 플러그인은 MS-PAC를 디코딩하고, 데이터를 확인하고, 필터링합니다. 로컬 그룹과 같은 추가 정보로 MS-PAC를 보강해야 하는지 확인하기 위해 LDAP 서버에서 조회를 수행합니다.
8. 그런 다음 IPA-KDB 플러그인은 PAC를 인코딩하고 서명하여 서비스 티켓에 연결한 다음 AD 클라이언트로 보냅니다.

9. 이제 AD 클라이언트에서 IdM requirements에서 발행한 서비스 티켓을 사용하여 IdM 서비스에 연결할 수 있습니다.

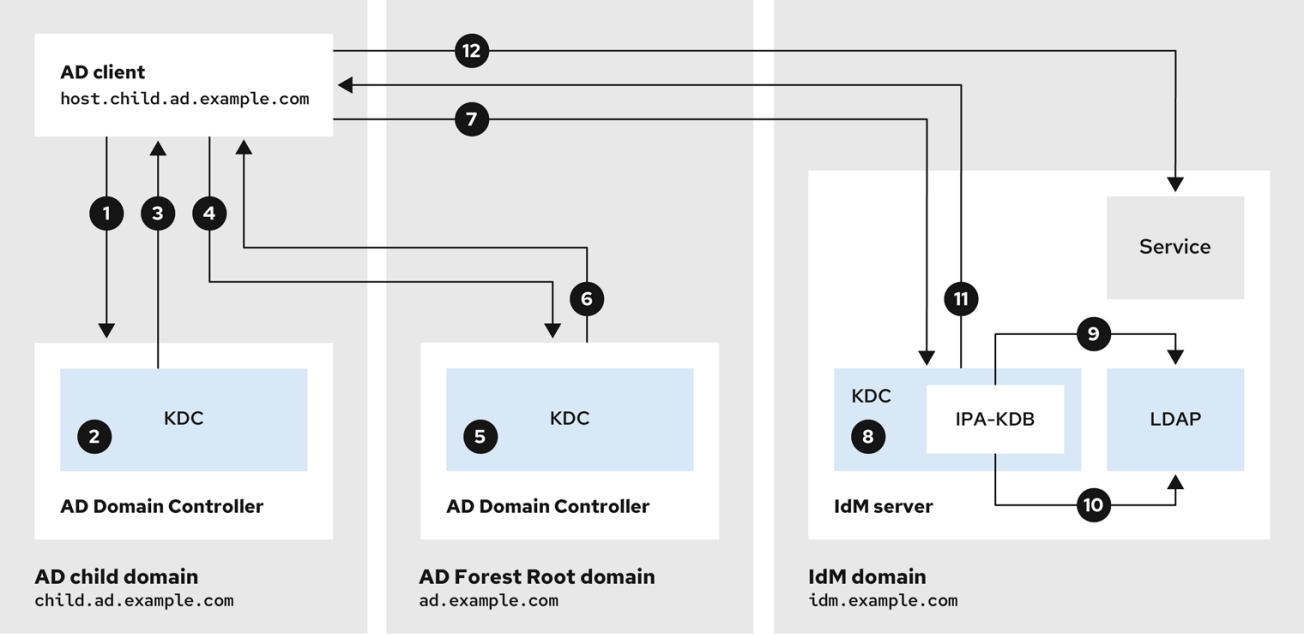
추가 리소스

- AD 하위 도메인의 호스트가 IdM 서버에서 서비스를 요청하는 경우 정보 흐름

11.2. AD 하위 도메인의 호스트가 IDM 서버에서 서비스를 요청하는 경우 정보 흐름

다음 다이어그램에서는 하위 도메인의 AD(Active Directory) 호스트가 IdM(Identity Management) 도메인의 서비스를 요청할 때 정보 흐름을 설명합니다. 이 시나리오에서는 AD 클라이언트가 하위 도메인의 KDC(Kerberos 배포 센터)에 접속한 다음, AD forest root의 EgressIP에 연결하고, 마지막으로 IdM 서비스에 대한 액세스를 요청하도록 IdM()에 연결합니다.

AD 클라이언트에서 IdM 서비스에 액세스하는 데 문제가 있고 AD 클라이언트가 AD forest root의 하위 도메인인 도메인에 속하는 경우 이 정보를 사용하여 문제 해결 작업을 좁히고 문제 소스를 확인할 수 있습니다.



1. AD 클라이언트는 자체 도메인에서 AD Kerberos Distribution Center(KDC)에 연결하여 IdM 도메인에서 서비스에 대한 TGS 요청을 수행합니다.
2. 하위 도메인인 **child.ad.example.com** 의 AD EgressIP은 해당 서비스가 신뢰할 수 있는 IdM 도메인에 속하는지 인식합니다.
3. 하위 도메인의 AD EgressIP은 클라이언트에 AD forest root 도메인 **ad.example.com** 에 대한 추천 티켓을 보냅니다.
4. AD 클라이언트는 IdM 도메인의 서비스에 대한 AD forest 루트 도메인의 EgressIP에 연결합니다.
5. est 루트 도메인의 EgressIP은 서비스가 신뢰할 수 있는 IdM 도메인에 속하는 것을 인식합니다.
6. AD EgressIP은 클라이언트에 신뢰할 수 있는 IdM key에 대한 참조와 함께 TGT(cross-realm ticket-granting ticket)를 클라이언트에 보냅니다.

7. AD 클라이언트는 cross-realm TGT를 사용하여 IdM EgressIP에 티켓을 요청합니다.
8. IdM EgressIP은 교차 실제 TGT와 함께 전송된 Privileged Attribute Certificate (MS-PAC)의 유효성을 검사합니다.
9. IPA-KDB 플러그인은 LDAP 디렉토리를 확인하여 요청된 서비스에 대한 티켓을 받을 수 있는 외부 주체가 허용되는지 확인할 수 있습니다.
10. IPA-KDB 플러그인은 MS-PAC를 디코딩하고, 데이터를 확인하고, 필터링합니다. 로컬 그룹과 같은 추가 정보로 MS-PAC를 보강해야 하는지 확인하기 위해 LDAP 서버에서 조회를 수행합니다.
11. 그런 다음 IPA-KDB 플러그인은 PAC를 인코딩하고 서명하여 서비스 티켓에 연결한 다음 AD 클라이언트로 보냅니다.
12. 이제 AD 클라이언트에서 IdM requirements에서 발행한 서비스 티켓을 사용하여 IdM 서비스에 연결할 수 있습니다.

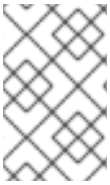
추가 리소스

- AD forest 루트 도메인의 호스트가 IdM 서버에서 서비스를 요청할 때 정보 흐름

11.3. IDM 클라이언트가 AD 서버에서 서비스를 요청할 때 정보 흐름

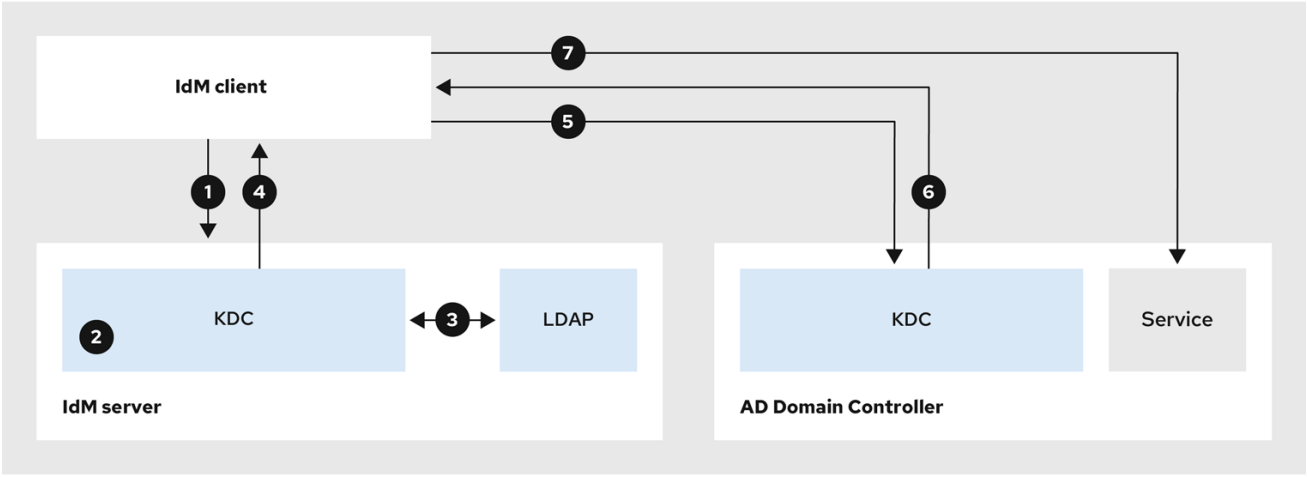
다음 다이어그램에서는 IdM(Identity Management) 클라이언트가 IdM과 AD 간 양방향 신뢰를 구성한 경우 AD(Active Directory) 도메인의 서비스를 요청할 때 정보 흐름을 설명합니다.

IdM 클라이언트의 AD 서비스에 액세스하는 데 문제가 있는 경우 이 정보를 사용하여 문제 해결 노력을 좁히고 문제 소스를 확인할 수 있습니다.



참고

기본적으로 IdM은 AD에 대한 단방향 트러스트를 설정하여 AD의 리소스에 대해 TGT(cross-realm ticket-granting ticket)를 발행할 수 없음을 의미합니다. 신뢰할 수 있는 AD 도메인에서 서비스에 티켓을 요청하려면 양방향 트러스트를 구성합니다.



231_RHEL_0422

1. IdM 클라이언트는 연락처를 원하는 AD 서비스를 위해 IdM KDC(Keranting Center)에서 티켓 통합 티켓(TGT)을 요청합니다.

2. *IdM EgressIP은 서비스가 AD 영역에 속하고, 영역이 알려진지, 신뢰할 수 있고 클라이언트가 해당 영역에서 서비스를 요청할 수 있는지 확인합니다.*

3. *IdM Directory Server의 사용자 주체에 대한 정보를 사용하여 IdM EgressIP은 사용자 주체에 대한 권한 있는 속성 인증서(MS-PAC) 레코드가 포함된 교차 실제 TGT를 생성합니다.*

4. *IdM key는 IdM 클라이언트에 교차 실제 TGT를 다시 보냅니다.*

5. *IdM 클라이언트는 AD EgressIP에 연결하여 IdM XX에서 제공하는 MS-PAC가 포함된 교차 영역 TGT를 제공하는 AD 서비스 티켓을 요청합니다.*

6. *AD 서버는 PAC의 유효성을 검증 및 필터링하고 AD 서비스에 대한 티켓을 반환합니다.*

7. *IPA 클라이언트에서 이제 AD 서비스에 연결할 수 있습니다.*

추가 리소스

- *단방향 신뢰 및 양방향 신뢰*

12장. 명령줄을 사용하여 신뢰 제거

명령줄 인터페이스를 사용하여 IdM 측에서 IdM(Identity Management)/Active Directory(AD) 신뢰를 제거하려면 다음 절차를 따르십시오.

사전 요구 사항

- IdM 관리자로 Kerberos 티켓을 받았습니다. 자세한 내용은 웹 UI의 Logging to IdM을 참조하십시오. Kerberos 티켓 사용.

절차

1. **ipa trust-del** 명령을 사용하여 IdM에서 신뢰 구성을 제거합니다.

```
[root@server ~]# ipa trust-del ad_domain_name
-----------------------------
Deleted trust "ad_domain_name"
-----------------------------
```

2. Active Directory 구성에서 trust 개체를 제거합니다.

참고

신뢰 구성을 제거해도 AD 사용자에 대해 IdM이 생성된 ID 범위가 자동으로 제거되지는 않습니다. 이렇게 하면 신뢰를 다시 추가하면 기존 ID 범위가 다시 사용됩니다. 또한 AD 사용자가 IdM 클라이언트에서 파일을 생성한 경우 해당 POSIX ID는 파일 메타데이터에 보존됩니다.

AD 신뢰와 관련된 모든 정보를 제거하려면 신뢰 구성 및 신뢰 개체를 제거한 후 AD 사용자 ID 범위를 제거하십시오.

```
# ipa idrange-del AD.EXAMPLE.COM_id_range
# systemctl restart sssd
```

검증 단계

- **ipa trust-show** 명령을 사용하여 신뢰가 제거되었는지 확인합니다.

```
[root@server ~]# ipa trust-show ad.example.com
ipa: ERROR: ad.example.com: trust not found
```

추가 리소스

- AD에 대한 트러스트를 제거한 후 ID 범위 제거

13장. IDM 웹 UI를 사용하여 신뢰 제거

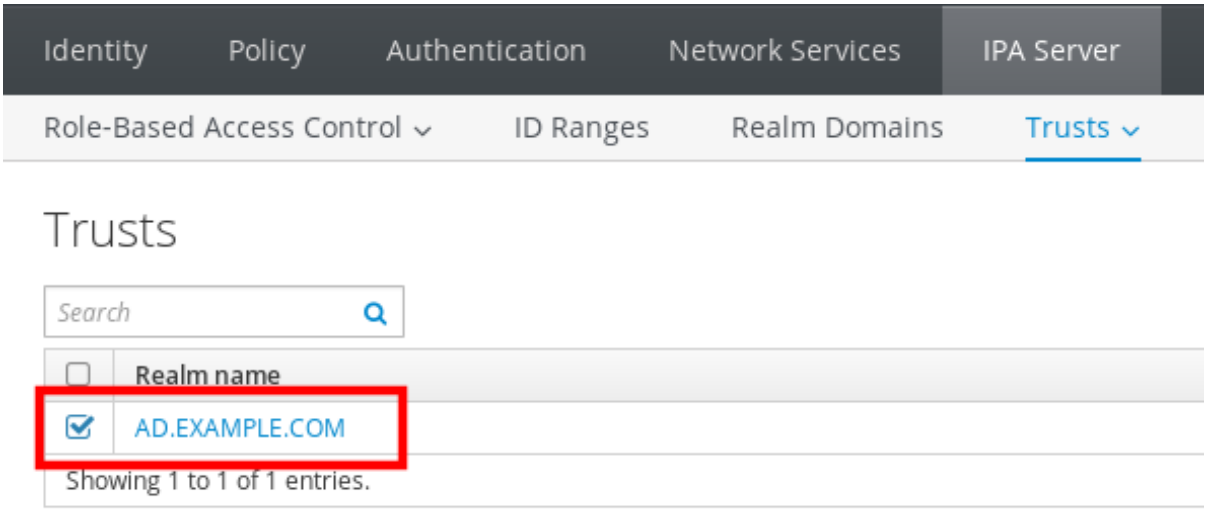
IdM 웹 UI를 사용하여 IdM(Identity Management)/AD(Active Directory) 신뢰를 제거하려면 다음 절차를 따르십시오.

사전 요구 사항

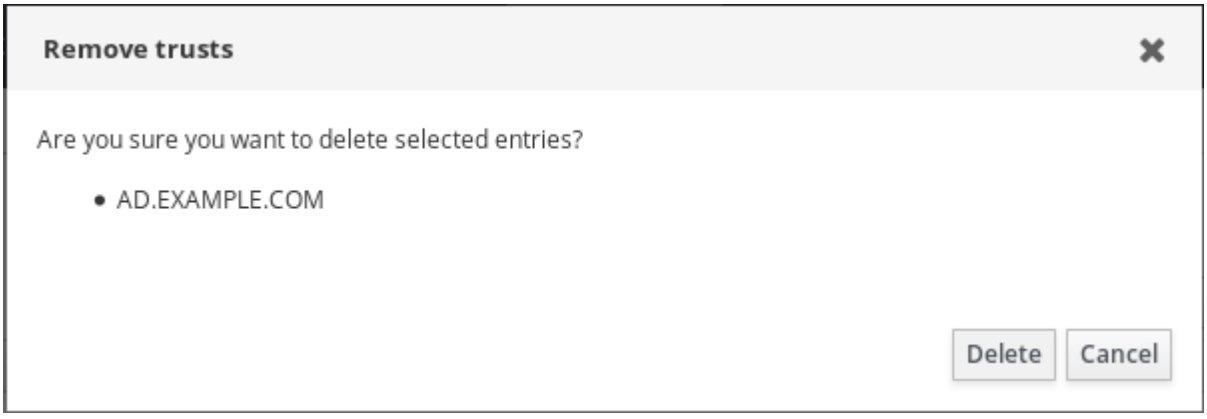
- Kerberos 티켓을 받았습니다. 자세한 내용은 웹 UI의 Logging to IdM을 참조하십시오. Kerberos 티켓 사용.

절차

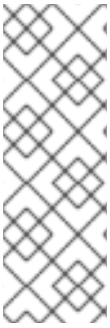
1. 관리자 권한으로 IdM 웹 UI에 로그인합니다. 자세한 내용은 웹 브라우저에서 IdM 웹 UI 액세스를 참조하십시오.
2. IdM 웹 UI에서 **IPA 서버** 탭을 클릭합니다.
3. **IPA 서버** 탭에서 신뢰 탭을 **클릭합니다**.
4. 제거할 신뢰를 선택합니다.



5. **삭제** 버튼을 클릭합니다.
6. **신뢰 제거** 대화 상자에서 **삭제** 를 클릭합니다.



7. Active Directory 구성에서 trust 개체를 제거합니다.



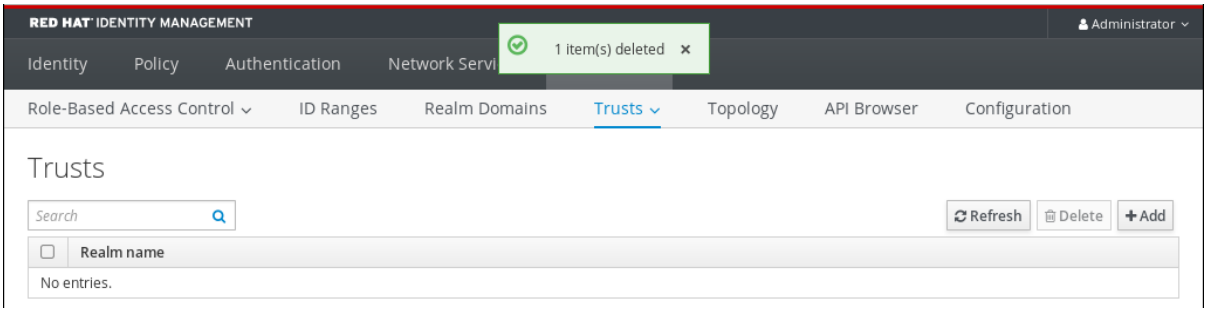
참고

신뢰 구성을 제거해도 AD 사용자에 대해 IdM이 생성된 ID 범위가 자동으로 제거되지는 않습니다. 이렇게 하면 신뢰를 다시 추가하면 기존 ID 범위가 다시 사용됩니다. 또한 AD 사용자가 IdM 클라이언트에서 파일을 생성한 경우 해당 POSIX ID는 파일 메타데이터에 보존됩니다.

*AD 신뢰와 관련된 모든 정보를 제거하려면 신뢰 구성 및 신뢰 오브젝트를 제거한 후 **ID 범위** 탭에서 AD 사용자 ID 범위를 제거하십시오.*

검증 단계

- *신뢰가 성공적으로 삭제되면 웹 UI에 텍스트가 포함된 녹색 팝업이 표시됩니다.*



추가 리소스

- *AD에 대한 트러스트를 제거한 후 ID 범위 제거*

14장. ANSIBLE을 사용하여 신뢰 제거

Ansible 플레이북을 사용하여 IdM 측에서 IdM(Identity Management)/Active Directory(AD) 신뢰를 제거하려면 다음 절차를 따르십시오.

사전 요구 사항

- IdM 관리자로 Kerberos 티켓을 받았습니다. 자세한 내용은 웹 UI의 Logging to IdM을 참조하십시오. Kerberos 티켓 사용.
- 다음 요구 사항을 충족하도록 Ansible 제어 노드를 구성했습니다.
  - Ansible 버전 2.14 이상을 사용하고 있습니다.
  - Ansible 컨트롤러에 **ansible-freeipa** 패키지가 설치되어 있습니다.
  - 이 예제에서는 **~/MyPlaybook/** 디렉터리에서 IdM 서버의 정규화된 도메인 이름(FQDN)을 사용하여 Ansible 인벤토리 파일을 생성했다고 가정합니다.
  - 이 예제에서는 **secret.yml** Ansible 자격 증명 모음이 **ipaadmin_password** 를 저장하는 것으로 가정합니다.
- **ansible-freeipa** 모듈이 실행되는 노드인 대상 노드는 IdM 도메인의 일부인 IdM 클라이언트, 서버 또는 복제본입니다.

절차

1. **~/MyPlaybooks/** 디렉터리로 이동합니다.

```
$ cd ~/MyPlaybooks/
```

2. 다음 콘텐츠를 사용하여 **del-trust.yml** 플레이북을 생성합니다.

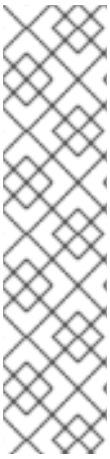
```
---
- name: Playbook to delete trust
  hosts: ipaserver

  vars_files:
  - /home/user_name/MyPlaybooks/secret.yml
  tasks:
    - name: ensure the trust is absent
      ipatrust:
        ipaadmin_password: "{{ ipaadmin_password }}"
        realm: ad.example.com
        state: absent
```

   예제에서 **realm** 은 AD 영역 이름 문자열을 정의합니다.

3. 파일을 저장합니다.

4. Ansible 플레이북을 실행합니다. Playbook 파일, **secret.yml** 파일을 보호하는 암호를 저장하는 파일, 인벤토리 파일을 지정합니다.

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory del-trust.yml
```



참고

신뢰 구성을 제거해도 AD 사용자에 대해 IdM이 생성된 ID 범위가 자동으로 제거되지는 않습니다. 이렇게 하면 신뢰를 다시 추가하면 기존 ID 범위가 다시 사용됩니다. 또한 AD 사용자가 IdM 클라이언트에서 파일을 생성한 경우 해당 POSIX ID는 파일 메타데이터에 보존됩니다.

AD 신뢰와 관련된 모든 정보를 제거하려면 신뢰 구성 및 신뢰 개체를 제거한 후 AD 사용자 ID 범위를 제거하십시오.

```
# ipa idrange-del AD.EXAMPLE.COM_id_range
# systemctl restart sssd
```

검증 단계

- ***ipa trust-show*** *명령을 사용하여 신뢰가 제거되었는지 확인합니다.*

```
[root@server ~]# ipa trust-show ad.example.com
ipa: ERROR: ad.example.com: trust not found
```

추가 리소스

- */usr/share/doc/ansible-freeipa/README-trust.md*
- */usr/share/doc/ansible-freeipa/playbooks/trust*
- *AD에 대한 트러스트를 제거한 후 ID 범위 제거*

15장. AD에 대한 트러스트를 제거한 후 ID 범위 제거

IdM 및 AD(Active Directory) 환경 간 신뢰를 제거한 경우 연결된 ID 범위를 제거할 수 있습니다.

주의

신뢰할 수 있는 도메인과 연결된 ID 범위에 할당된 ID는 IdM에 등록된 시스템에서 파일 및 디렉터리의 소유권에 계속 사용될 수 있습니다.

삭제한 AD 신뢰에 해당하는 ID 범위를 제거하면 AD 사용자가 소유한 파일 및 디렉터리의 소유권을 확인할 수 없습니다.

사전 요구 사항

- AD 환경에 대한 트러스트를 제거했습니다.

절차

1. 현재 사용 중인 모든 ID 범위를 표시합니다.

```
[root@server ~]# ipa idrange-find
```

2. 제거한 신뢰와 연결된 ID 범위의 이름을 식별합니다. ID 범위 이름의 첫 번째 부분은 신뢰의 이름입니다(예: **AD.EXAMPLE.COM_id_range**).

3. 범위를 제거합니다.

```
[root@server ~]# ipa idrange-del AD.EXAMPLE.COM_id_range
```

4. SSSD 서비스를 다시 시작하여 제거한 ID 범위에 대한 참조를 제거합니다.

```
[root@server ~]# systemctl restart sssd
```

추가 리소스

- 명령줄을 사용하여 신뢰 제거를 참조하십시오.
- IdM 웹 UI를 사용하여 신뢰 제거를 참조하십시오.